Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Aljoša Počič

Principi zaznavanja neželjenih dogodkov v večjih informacijskih sistemih

DIPLOMSKO DELO
UNIVERZITETNI ŠTUDIJSKI PROGRAM PRVE STOPNJE
RAČUNALNIŠTVO IN INFORMATIKA

prof. dr. Miha Mraz
MENTOR

Ljubljana, 2017

Tematika naloge:

Kandidat naj v svojem delu predstavi aktualne koncepte zaznavanja in analize neželjenih dogodkov v večjih informacijskih sistemih. Pri tem naj izpostavi trenutno aktualne tehnologije tega področja in na vzorčnem primeru informacijskega sistema prikaže njihovo uporabo.

IZJAVA O AVTORSTVU DIPLOMSKEGA DELA

Spodaj podpisani izjavljam, da sem avtor dela, da slednje ne vsebuje materiala, ki bi ga kdorkoli predhodno že objavil ali oddal v obravnavo za pridobitev naziva na univerzi ali drugem visokošolskem zavodu, razen v primerih kjer so navedeni viri.
S svojim podpisom zagotavljam, da:

- sem delo izdelal samostojno pod mentorstvom prof. dr. Mihe Mraza,
- so elektronska oblika dela, naslov (slov., angl.), povzetek (slov., angl.) ter ključne besede (slov., angl.) identični s tiskano obliko in
- soglašam z javno objavo elektronske oblike dela v zbirki "Dela FRI".

— Aljoša Počič, Ljubljana, september 2017.

Univerza v Ljubljani
Fakulteta za računalništvo in informatiko

Aljoša Počič

Principi zaznavanja neželjenih dogodkov v večjih informacijskih sistemih

POVZETEK

Varnost v informacijskem okolju ni odvisna samo od uporabljenih tehnologij, temveč tudi od vpeljanih politik in pravil. Kot odgovor na pojav novih napadov in groženj, so se pojavile nove varnostne zaščite. Da lahko izkoristimo podatke pridobljene s strani različnih varnostnih zaščit in vpeljemo politke v vsakodnevne aktivnosti znotraj informacijskega sistema, uporabimo SIEM sistem. SIEM sistem prevzame centralno vlogo v varnosti informacijskega sistema. Vsi zapisi, dogodki in mrežni promet se hranijo na enotnem mestu v normalizirani obliki, ki omogoča analizo njihove korelacije. S tem pridobimo centralno mesto iz katerega lahko spremljamo stanje varnosti v informacijskem sistemu in izvajamo analize ter poročila iz področja varnosti. V diplomskem delu so opisani ključni viri podatkov za SIEM sisteme in možnosti pridobivanja podatkov iz mrežnega prometa. Opisan je razvoj SIEM sistemov skozi čas in pričakovanja od današnjih SIEM sistemov naslednje generacije.

V nadaljevanju dela sta podrobneje opisana vzorčni naročnik SIEM sistema in njegovo okolje. Navedene in opisane so vrste naprav v okolju naročnika in integracija naprav v uporabljeni SIEM sistem. V zaključku naloge je prikazana uporaba rešitve in tri tipična področja analiz, ki se izvajajo v SIEM sistemu. Za analizo iskanja naprednih napadov je prikazana tudi uporaba brezplačnih spletnih orodij, s katerimi lahko potrdimo ali ovržemo zaznave ugotovljene s strani varnostnih rešitev v informacijskem okolju.

Ključne besede: SIEM, varovanje informacijske infrastrukture, zapisi, dogodki, korelacije, varnost

University of Ljubljana
Faculty of Computer and Information Science

Aljoša Počič

Detection of critical events in complex information systems

ABSTRACT

Safety in the information environment depends not just on the technologies used, but also on the policies and rules in place. New security protections have developed as a response to new threats and attacks. In order to make use of the data obtained from different security protections and introduce policies into everyday activities within the information system, we used a SIEM system. SIEM system assumes the essential role regarding security of the information system. All records, events and network traffic are stored in one place and in a normalized form, which allows analysis of their correlation. This is how we gain a central position, allowing us to monitor the security situation in the information system, and also to conduct analyses and security reports. The thesis discusses the key sources of information for SIEM systems and the possibilities for data collection from the network traffic. The development of SIEM systems over time and the expectations of next generation SIEM systems available today are also described.

The following part focuses on the sample customer and on the model environment. The types of devices in the customer's environment and the integration of devices in the SIEM system used are listed and described as well. The last part of the thesis shows the use of the solution and three typical areas of analyses performed in the SIEM system. The analysis of advanced attacks also shows the use of free online tools that help us to confirm or reject the threats identified by the security solutions in the information environment.

Key words: SIEM, protection of information infrastructure, logs, events, correlations, security

ZAHVALA

Zahvaljujem se mentorju prof. dr. Mihi Mrazu za pomoč, svetovanje in vodenje pri izdelavi diplomskega dela. Zahvaljujem se tudi družini za vzpodbude in priganjanje, sedaj je pa že res čas.

— Aljoša Počič, Ljubljana, september 2017.

KAZALO

1 Uvod

Varnost v informacijskem okolju je v zadnjih letih zaradi več dejavnikov postala eno od ključnih področij, s katerim se srečujejo organizacije. Če je še nekaj let nazaj veljalo, da morajo v varnost informacijskega okolja vlagati predvsem banke, zavarovalnice, javna uprava ipd., danes to velja za vse organizacije, ki uporabljajo svetovni splet ali elektronsko komunikacijo. Eden od dejavnikov sta zakonodaja in regulativa, kjer so z zakoni in predpisi navedene zahteve za določene organizacije. Primer takšnega zakona je Zakon o varovanju osebnih podatkov. Drugi od dejavnikov je razmah izsiljevalskih virusov v zadnjih letih, katerih žrtve so ne samo organizacije, ampak tudi fizične osebe. Tretji pomembnejši dejavnik je vse večja vpletenost informacijskega okolja v poslovni proces. Tako lahko vdor v informacijski sistem pomeni izgubo podatkov kritičnih za poslovni proces in izgubo konkurenčne prednosti podjetja. Z naraščanjem vpletenosti informacijskega okolja v poslovni proces, je to okolje postalo zanimivo za napadalce, katerih namen je pridobitev informacij, ki jih lahko prodajo na trgu. Ker se je spremenil tip napadalcev, ki so sedaj bolje izobraženi in pripravljeni investirati večje količine denarja v izvedbo napada, se morajo temu prilagoditi tudi organizacije z varovanjem svojega informacijskega

okolja. Del teh prilagoditev je povezan na vpeljavo novih varnostnih rešitev, del pa tudi na vpeljavo procesov in izobraževanj iz področja varnosti.

Vpeljava novih varnostnih rešitev na eni strani in priprava pravilnikov ali celo varnostnih politik na drugi, ni zadovoljivo rešila novih varnostnih izzivov. Izkazalo se je, da manjka povezovalni člen med tehnologijo in pravili. Zato smo v diplomski nalogi predstavili orodje za spemljanje stanja varnosti v informacijskem okolju. Gre za rešitev SIEM, ki je po našem mnenju povezovalni element med informacijskimi sistemi in procesi iz področja informacijske varnosti. Tehnološko gledano gre za še eno IT napravo, ki zbira in procesira zapise iz različnih virov. Ko tej napravi dodamo logiko korelacij, poslovno kritičnost naprav in pravila uporabe informacijskih virov, dobimo povezovalni člen med tehnologijami in politikami oziroma pravilniki. Dodatno nam SIEM sistem s svojo centralizacijo poenostavi spremljanje stanja v informacijskem okolju in pohitri zaznavo okuženega sistema znotraj okolja.

V drugem poglavju govorimo o načinih, kako spremljati stanje varnosti v informacijskem okolju. Predstavljeni so različni načini beleženja sistemskih in aplikativnih dogodkov na najbolj tipičnih napravah, ki jih srečamo v informacijskem okolju. Predstavljeni so postopki spremljanja mrežnega prometa in načini preverjanja virov informacij na svetovnem spletu in orodjih za varnostno analizo datotek. V tretjem poglavju govorimo o načinih zbiranja, pregledovanja in koreliranja zapisov. Opišemo zgodovino SIEM sistemov in njihov razvoj do danes. Navedene in opisane so funkcionalnosti, ki jih pričakujemo od SIEM sistemov naslednje generacije in kaj je njihov namen na področju varnosti informacijskega okolja. V četrtem poglavju govorimo o načinu implementacije SIEM sistema v vzorčno okolje. Opisan je naročnik in vzorčno okolje, navedeni so tipi naprav, ki se uporabljajo in njihovo število ter funkcionalnosti. Opisana je uporabljena SIEM rešitev in povezava virov vanjo. Predstavljene so tri tipične skupine situcij, ki jih srečamo pri uporabi SIEM sistema. Podrobno so prikazani postopki, kako se uporabnik SIEM sistema loti pregledovanja stanja in vrtanja v globino. Zadnji primer opisuje tudi način uporabe spletnih orodij, ki so praviloma prosto dostopna in lahko ponudijo dodatno razumevanje dogodkov, ki jih zabeležijo sistemi v informacijskem okolju.

2 Spremljanje stanja varnosti v informacijskem okolju

2.1 Uvod

V sodobnem informacijskem okolju se srečujemo z različnimi napravami, programsko opremo in storitvami, ki jih bodisi nudimo, bodisi koristimo v svetovnem spletu. Prav tako se srečujemo z različnimi vrstami in vlogami uporabnikov, ki imajo različna dovoljenja pri dostopu do storitev in podatkov. Informacijsko okolje je zelo dinamično in stalno spreminjajoče. Skrbnik okolja, zadolžen za varnost, je tako postavljen pred zahtevno nalogo ščitenja informacijskih sredstev pred zunanjimi in notranjimi informacijskimi nevarnostmi, ki so lahko namerne ali pa naključne. Skrbnik tako želi vedeti, kakšno je stanje varnosti v njegovem okolju v določenem trenutku. V primeru ugotovljenega varnostnega incidenta poleg odprave posledic incidenta želi izvedeti tudi podatke o tem kako in kdaj je do njega prišlo, kdo je bil poleg odkritega še udeležen pri istem incidentu in kakšno je bilo obnašanje kompromitiranega sistema v informacijskem okolju.

Čedalje več okolij se zaveda pomena informacijske varnosti in varovanja poslovnih informacij, informacij o strankah, zaposlenih, poslovnih partnerjih itd. Z rastjo zavedanja pomena varnosti so se izvedle investicije v različne varnostne rešitve kot so požarne pre-

grade naslednje generacije (angl. *Next Generation Firewall -NGFW*), zaščita klientov, naprave za preverjanje SSL prometa, kontrole dostopa do omrežja itd.
Posamezna zaščita varuje le pred določenimi tipi napadov in za celovit pogled v stanje informacijskega okolja je potrebna analiza in iskanje povezav med dogodki zaznanimi s strani različnih sistemov. Pri tem opravilu nam pomagajo zapisi, ki jih generirajo posamezni sistemi in naprave. Zapisi se lahko nahajajo na lokalnem sistemu ali napravi, če pa jih želimo korelirati med seboj, je smiselno centralno zbiranje na namenskem sistemu. Včasih sistem iz različnih razlogov ne zabeleži aktivnosti, ki bi jo v analizi incidenta potrebovali, zato je smiselno spremljati tudi mrežni promet (vsaj) do kritičnih informacijskih sistemov. Lahko se zgodi, da moramo zabeleženo informacijo oplemenititi ali preveriti z informacijami pridobljenimi iz svetovnega spleta. Slednje lahko izvajamo z integracijo sistema iz našega okolja v oblačni sistem, ali pa z ročnim pridobivanjem informacij iz svetovnega spleta.

2.2 Beleženje sistemskih dogodkov

Dnevniški zapis (krajše zapis) je samodejno zabeleženo in časovno žigosano dokumentiranje dogodka, ki se je zgodil na določenen sistemu [1]. Informacijski sistemi že od nekdaj omogočajo beleženje različnih sistemskih, aplikativnih in uporabniških dogodkov oziroma aktivnosti. Beleženje se lahko izvaja na ekran (konzolo), interni pomnilnik, datoteko ali posreduje na zunanji sistem, ki je običajno “Syslog” oziroma “SNMP” strežnik.
Zabeleženi zapisi lahko vsebujejo podatke s pomočjo katerih zaznamo nepravilnosti v delovanju sistema, aplikacije ali uporabnika. Služijo nam lahko za sledenje aktivnostim uporabnika pri delu s sistemom, spremljanje delovanja sistemskih in aplikacijskih servisov ter spremljanje delovanja sistema. Posamezen zapis se tako lahko nanaša na različne dogodke, ki so se zgodili v sistemu. Praviloma se nanaša na beleženje napak ali opozoril na sistemih, lahko pa se uporablja za sledenje izvajanju sistemskih ukazov, prijavam in odjavam na sistem itd. Izziv predstavlja dejstvo, da ima vsak sistem beleženja svojo strukturo zapisa. Večina bolj naprednih sistemov omogoča nastavitev nivoja beleženja od obveščanja samo o kritičnih dogodkih preko informativnih dogodkov vse do podrobnega beleženja vsega, kar se dogaja na sistemu. Različne nastavitve nivojev beleženja so prikazane na sliki 2.1.

Posamezna naprava zapisuje dogodke kot jih vidi glede na vlogo, ki jo opravlja v

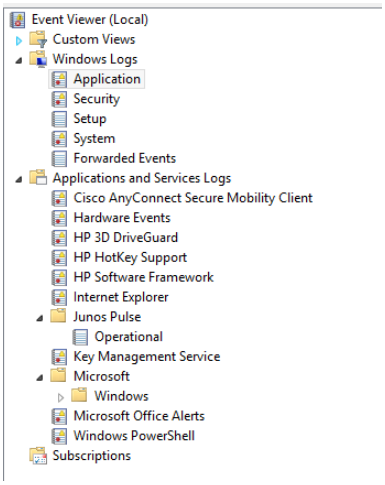
Level Keyword	Level	Description	Syslog Definition
emergencies	0	System unusable	LOG_EMERG
alerts	1	Immediate action needed	LOG_ALERT
critical	2	Critical conditions	LOG_CRIT
errors	3	Error conditions	LOG_ERR
warnings	4	Warning conditions	LOG_WARNING
notifications	5	Normal but significant condition	LOG_NOTICE
informational	6	Informational messages only	LOG_INFO
debugging	7	Debugging messages	LOG_DEBUG

Slika 2.1 Primer nastavitev nivojev beleženja na Cisco usmerjevalnikih [2].

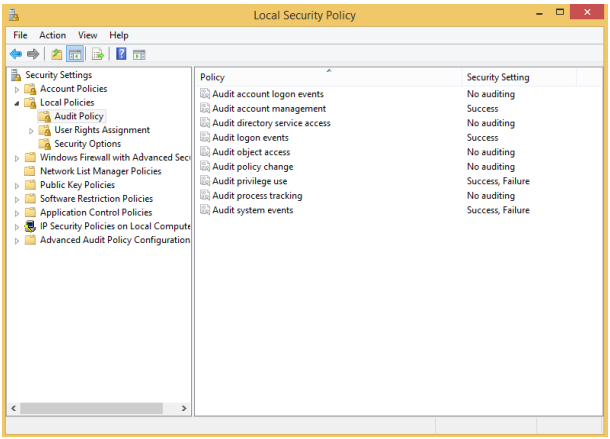
informacijskem sistemu. S koreliranjem zapisov iz različnih virov lahko povežemo različne zapise v povezano celoto in zaznamo kompleksne varnostne dogodke. Z dodajanjem vsebin iz spletnih sistemov ter analizo sumljivih datotek lahko odkrijemo tudi zgodovino in razlog okužbe ter njene posledice na delovanje sistema. Tako lahko na primer odkrijemo kdo vse je obiskal okuženo spletno stran ali prejel škodljivo priponko v elektronski pošti. V nadaljevanju so navedeni in opisani primeri beleženja sistemov, ki so najbolj pogosti v tipičnem informacijskem okolju.

2.2.1 Microsoft Windows operacijski sistemi

Velika večina klientov v informacijskem okolju uporablja Microsoft Windows operacijski sistem [3]. Beleženje dogodkov v Microsoft Windows operacijskih sistemih se izvaja v tako imenovani "Event Log". Razvijalci programske opreme, ki želijo zapisovati zapise v "Event Log", morajo uporabiti tako imenovani "Instrumentation Manifest", katerega shemo specificira Windows Event Log API. "Instrumentation manifest" opredeli ponudnika in vsebino, ki se zapisuje v "Event log" ter vsebuje funkcije, ki so na voljo uporabnikom "Event loga" za branje in prikazovanje dogodkov. Najbolj znan prikazovalnik je Event Viewer. Obstajata dve kategoriji zapisov in sicer zapisi Windows sistema ter zapisi aplikacij in sistemskih servisov. Obe glavni kategoriji se nato delita na več podkategorij, kot je prikazano na sliki 2.2. V "Event Log" se beležijo sistemski dogodki potrebni za spremljanje in odpravljanje težav na nivoju operacijskega sistema, gonilnikov in aplikacij. Spremljajo se lahko tudi aktivnosti uporabnikov in procesov, kot so prijava in odjava iz sistema, uporaba priviligiranih dostopov in ukazov itd. Nivo beleženja sistemskih aktivnosti je odvisen od sistemskih nastavitev kot sta na primer "Audit policy" in "Security



Slika 2.2 Primer kategorij v Event Logu na Windows 10 operacijskem sistemu.



Slika 2.3 Primer nastavitev Audit policy na Windows 10 operacijskem sistemu.

Options" v varnostnih nastavitvah operacijskega sistema, kar je prikazano na sliki 2.3.

2.2.2 Linux operacijski sistemi

Pogosteje kot na klientih se z Linux operacijskimi sistemi srečamo na strežnikih [4]. Zapisi Linux sistemov se praviloma nahajajo v mapi /var/log in njenih podmapah. Zapisi so večinoma v ASCII obliki in jih lahko pregledujemo s sistemskimi ukazi kot so more, cat, less, tail in podobni. Izjema sta datoteki wtmp in utmp, ki vsebujeta podatke o aktivnostih uporabnika in ju lahko pregledujemo z ukazi kot sta last ali utmpdump. Tudi Linux sistemi omogočajo prilagajanje nivoja zapisovanja in datoteko v katero se le to izvaja. Primeri različnih nastavitev logiranja pri Linux operacijskem sistemu so navedeni

v zapisu 2.1.

Zapis 2.1 Nastavitve logiranja pri Linux operacijskem sistemu.

```
# Logiraj vse na nivoju info razen elektronske poste in cron procesa
# Logiraj v datoteko messages
 *.info;mail.none;cron.none /var/log/messages
# Logiraj vso elektronsko posto v maillog datoteko
mail.*  /var/log/maillog
# Zapisuj vsa sporocila jedra na konzolo
kern.*  /dev/console
```

2.2.3 Beleženje požarnih pregrad

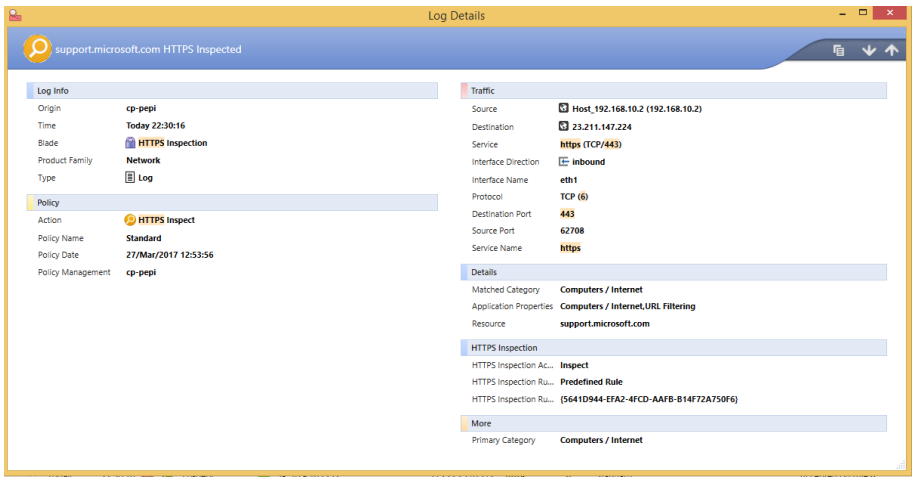
Naprednejše požarne pregrade omogočajo več različnih vrst beleženja, kot so beleženje zaznanih dogodkov, zaznanega prometa, beleženje aktivnosti oddaljenih uporabnikov in administratorjev pa vse do sistemskih dogodkov, kot so ustavitev ali zagon servisov, posodobitev baz zapisov, aktivnosti uporabnikov na nivoju operacijskega sistema itd. Zaradi količine števila zapisov je pomembno, da se za beleženje uporablja podatkovna baza, ki omogoča tudi hitro iskanje zabeleženih dogodkov in "vrtanje" v globino pri analizi dogajanja v sistemu. Podatki, ki jih beležijo požarne pregrade, praviloma vsebujejo vsaj naslednje informacije:

- izvor prometa (IP naslov ali uporabnik),
- izvorni port,
- cilj prometa (IP naslov, spletna stran),
- ciljni port,
- aplikacijo ali protokol,
- čas trajanja seje in količina prenešenih podatkov,
- preslikavo prometa (izvor, cilj ali port),
- akcijo (dovoljen ali blokiran promet).

Primer zapisa požarne pregrade Check Point 77.30 je predstavljen na sliki 2.4.

2.2.4 Beleženje poštnega sistema

Elektronska pošta velja za enega od večjih virov okužb prejetih iz svetovnega spleta in kot glavni komunikacijski kanal nenamernega odtekanja poslovnih informacij iz informacijskega okolja. Zaradi tega je še posebej pomembno beleženje prehoda elektronske pošte



Slika 2.4 Primer zapisa požarne pregrade Check Point pri pregledovanju https seje.

v in iz informacijskega okolja. Sistemi za pregledovanje elektronske pošte omogočajo različne funkcionalnosti že od faze vzpostavljanja same SMTP seje. Te funkcionalnosti so sledeče:

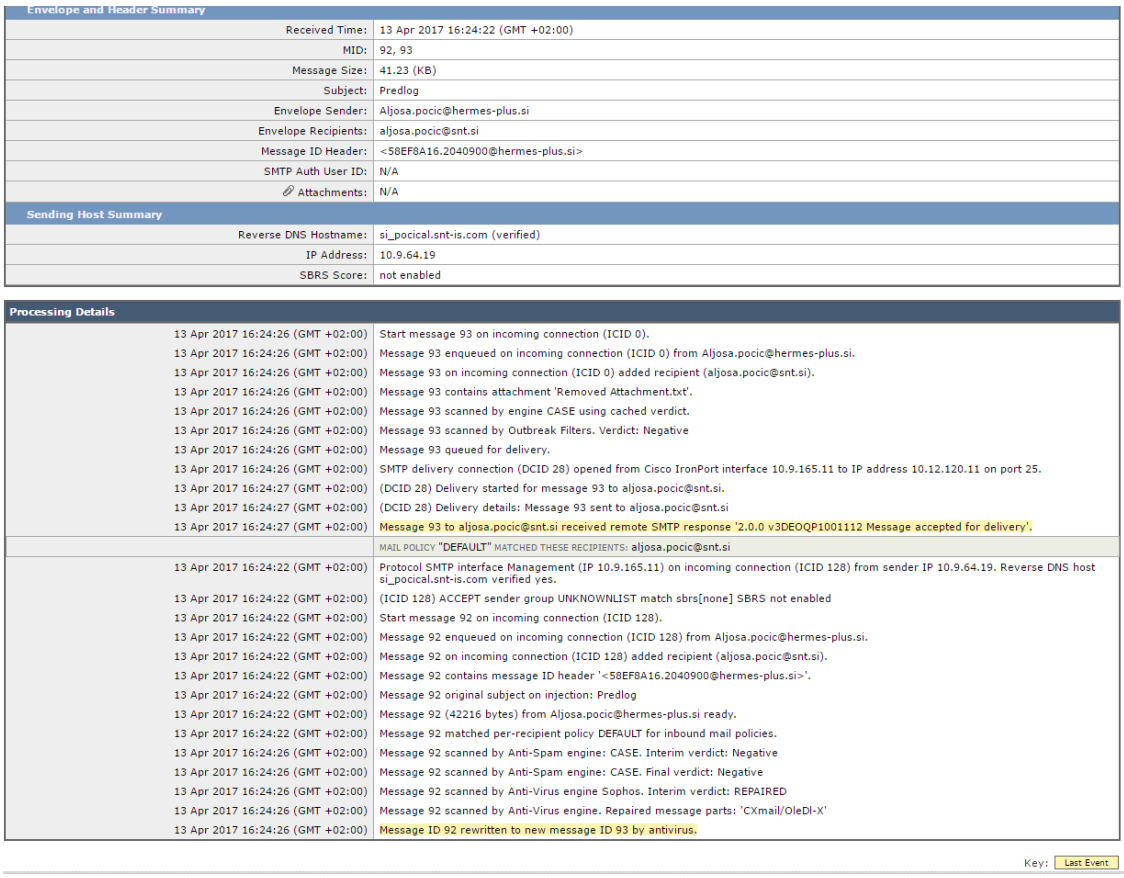
- preverjanje slovesa strežnika, ki pošilja elektronsko pošto,
- preverjanje DNS zapisov (SPF, DKIM, obstoječa domena, itd.),
- "greylisting".

Prav tako pa omogočajo pregledovanje vsebine sporočil in priponk v njih. Vrste pregledovanj vsebine sporočil so sledeče:

- "anti-virusno" pregledovanje,
- "anti-spam" pregledovanje,
- pregledovanje končnic in tipa priponk,
- pregledovanje vsebine sporočil.

Najbolj napredni poštni sistemi omogočajo celo preverjanje spletnih strani na katere kažejo povezave znotraj sporočila in integracjie z različnim sistemi za zaznavanje "neznanih napadov". Najpomembnejši podatki, ki se pričakujejo od zapisa pridobljenega iz poštnega sistema, so tako sledeči:

- IP naslov pošiljatelja,



Envelope and Header Summary

Received Time:	13 Apr 2017 16:24:22 (GMT +02:00)
MID:	92, 93
Message Size:	41.23 (KB)
Subject:	Predlog
Envelope Sender:	Aljosa.pocic@hermes-plus.si
Envelope Recipients:	aljosa.pocic@snt.si
Message ID Header:	<58EF8A16.2040900@hermes-plus.si>
SMTP Auth User ID:	N/A
Attachments:	N/A

Sending Host Summary

Reverse DNS Hostname:	si_pocical.snt-is.com (verified)
IP Address:	10.9.64.19
SBRS Score:	not enabled

Processing Details

13 Apr 2017 16:24:26 (GMT +02:00)	Start message 93 on incoming connection (ICID 0).
13 Apr 2017 16:24:26 (GMT +02:00)	Message 93 enqueued on incoming connection (ICID 0) from Aljosa.pocic@hermes-plus.si.
13 Apr 2017 16:24:26 (GMT +02:00)	Message 93 on incoming connection (ICID 0) added recipient (aljosa.pocic@snt.si).
13 Apr 2017 16:24:26 (GMT +02:00)	Message 93 contains attachment 'Removed Attachment.txt'.
13 Apr 2017 16:24:26 (GMT +02:00)	Message 93 scanned by engine CASE using cached verdict.
13 Apr 2017 16:24:26 (GMT +02:00)	Message 93 scanned by Outbreak Filters. Verdict: Negative
13 Apr 2017 16:24:26 (GMT +02:00)	Message 93 queued for delivery.
13 Apr 2017 16:24:26 (GMT +02:00)	SMTP delivery connection (DCID 28) opened from Cisco IronPort interface 10.9.165.11 to IP address 10.12.120.11 on port 25.
13 Apr 2017 16:24:27 (GMT +02:00)	(DCID 28) Delivery started for message 93 to aljosa.pocic@snt.si.
13 Apr 2017 16:24:27 (GMT +02:00)	(DCID 28) Delivery details: Message 93 sent to aljosa.pocic@snt.si
13 Apr 2017 16:24:27 (GMT +02:00)	Message 93 to aljosa.pocic@snt.si received remote SMTP response '2.0.0 v3DEOQP1001112 Message accepted for delivery'.
	MAIL POLICY "DEFAULT" MATCHED THESE RECIPIENTS: aljosa.pocic@snt.si
13 Apr 2017 16:24:22 (GMT +02:00)	Protocol SMTP interface Management (IP 10.9.165.11) on incoming connection (ICID 128) from sender IP 10.9.64.19. Reverse DNS host si_pocical.snt-is.com verified yes.
13 Apr 2017 16:24:22 (GMT +02:00)	(ICID 128) ACCEPT sender group UNKNOWNLIST match sbrs[none] SBRS not enabled
13 Apr 2017 16:24:22 (GMT +02:00)	Start message 92 on incoming connection (ICID 128).
13 Apr 2017 16:24:22 (GMT +02:00)	Message 92 enqueued on incoming connection (ICID 128) from Aljosa.pocic@hermes-plus.si.
13 Apr 2017 16:24:22 (GMT +02:00)	Message 92 on incoming connection (ICID 128) added recipient (aljosa.pocic@snt.si).
13 Apr 2017 16:24:22 (GMT +02:00)	Message 92 contains message ID header '<58EF8A16.2040900@hermes-plus.si>'.
13 Apr 2017 16:24:22 (GMT +02:00)	Message 92 original subject on injection: Predlog
13 Apr 2017 16:24:22 (GMT +02:00)	Message 92 (42216 bytes) from Aljosa.pocic@hermes-plus.si ready.
13 Apr 2017 16:24:22 (GMT +02:00)	Message 92 matched per-recipient policy DEFAULT for inbound mail policies.
13 Apr 2017 16:24:26 (GMT +02:00)	Message 92 scanned by Anti-Spam engine: CASE. Interim verdict: Negative
13 Apr 2017 16:24:26 (GMT +02:00)	Message 92 scanned by Anti-Spam engine: CASE. Final verdict: Negative
13 Apr 2017 16:24:26 (GMT +02:00)	Message 92 scanned by Anti-Virus engine Sophos. Interim verdict: REPAIRED
13 Apr 2017 16:24:26 (GMT +02:00)	Message 92 scanned by Anti-Virus engine. Repaired message parts: 'CXmail/OleDl-X'
13 Apr 2017 16:24:26 (GMT +02:00)	Message ID 92 rewritten to new message ID 93 by antivirus.

Key: Last Event

Slika 2.5 Primer zapisa programske opreme Cisco ESA verzije 10.0.1.

- pošiljatelj sporočila,
- prejemnik sporočila,
- priponke v sporočilu,
- podatki o sprejemu in dostavi sporočila,
- podatki o rezultatu varnostnih preverjanj.

Primer zapisa Cisco Email Security Appliance programske opreme je predstavljen na sliki 2.5.

2.2.5 Beleženje namestniškega strežnika

Namestniški strežnik (angl. *Proxy server*) je program, ki ima vlogo posredovanja zahtev in odgovorov med klienti iz lokalnega omrežja in svetovnim spletom. Eden od prvotnih

razlogov za uporabo namestniškega strežnika za dostop do svetovnega spleta je bila njegova sposobnost shranjevanja vsebine v svojem medpolnilniku in s tem manjša poraba pasovne širine proti internetu. Danes pa so veliko bolj pomembne njegove zmožnosti vsebinskega pregledovanja spletnega prometa. Te so sledeče:

- anti-virusno pregledovanje,
- filtriranje spletnih strani,
- kontrola aplikacij,
- dekriptiranje SSL prometa,
- pregledovanje vsebine, ki se prenaša v in iz svetovnega spleta.

Beleženje namestniških strežnikov je tako sestavljeno iz različnih sistemskih zapisov, zapisov povezanih s spremljanjem dela administratorjev sistema in beleženjem spletnih dostopov. Najpomembnejši podatki, ki se pričakujejo od zapisa pridobljenega iz namestniškega sistema, so tako sledeči:

- izvor prometa (IP naslov ali uporabnik),
- ciljni naslov (URL),
- uspešnost dostopa do ciljnega naslova,
- količina prenešenih podatkov,
- uporabljen klient,
- uporabljena metoda,
- podatki o rezultatu varnostnih preverjanj.

Primer zapisa McAfee Web Gateway programske opreme je predstavljen v zapisu 2.2.

Zapis 2.2 Primeri zapisov namestniškega strežnika MWG verzije 7.5

```
[19/Sep/2017:07:12:18 +0200] "" 10.12.64.9 200 "POST http://ocsp.digicert.com/ HTTP/1.1" ""
    "-" "" 887 460 "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox
    /55.0" "" "0" ""
[19/Sep/2017:07:12:18 +0200] "" 10.12.64.9 200 "GET http://pro.hit.gemius.pl/hmapxy.js HTTP
    /1.1" "" "-" "" 22760 331 "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101
    Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:18 +0200] "" 10.12.64.9 200 "GET http://24ur.com/lbin/registration2/sso_get
    .php?callback=jQuery172079858458579866 33_1505797938163&referer=
```

```
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://script.dotmetrics.net/door.js?id
    =1810 HTTP/1.1" "" "-" "" 8010 553 "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko
    /20100101 Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://www.dominvrt.si/static/slo/main/img
    /send_comments_ajax_loader.gif HTTP/1.1" "" "-" "" 3584 367 "Mozilla/5.0 (Windows NT
    10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://www.dominvrt.si/static/slo/
    messaging/img/more_ajax_loader.gif HTTP/1.1" "" "-" "" 1098 363 "Mozilla/5.0 (Windows NT
    10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://www.dominvrt.si/static/shared/img/
    ajax.gif HTTP/1.1" "" "-" "" 1832 344 "Mozilla/5.0 (Windows NT 10.0; WOW64; rv:55.0)
    Gecko/20100101 Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://www.dominvrt.si/static/slo/
    microsites/homeandgarden/img/poll_results_dot.png HTTP/1.1" "" "-" "" 504 378 "Mozilla
    /5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://images.24ur.com/media/images/108x60
    /Dec2015/61715041.jpg?d41d HTTP/1.1" "" "-" "" 3919 802 "Mozilla/5.0 (Windows NT 10.0;
    WOW64; rv:55.0) Gecko/20100101 Firefox/55.0" "" "0" ""
[19/Sep/2017:07:12:20 +0200] "" 10.12.64.9 200 "GET http://www.dominvrt.si/static/slo/
    microsites/vreme/img/map-icons/weather/OBLAK.png HTTP/1.1" "" "-" "" 11083 377 "Mozilla
    /5.0 (Windows NT 10.0; WOW64; rv:55.0) Gecko/20100101 Firefox/55.0" "" "0" ""
```

2.2.6 Beleženje varnostnega pregledovalnika sistemov

Varnostni pregledovalniki sistemov nam omogočajo pregledovanje informacijskega okolja z namenom zaznave uporabljenih sistemov in nudenih storitev ter iskanjem ranljivosti znotraj najdenih sredstev. V preteklosti so jih pretežno uporabljali pregledovalci varnosti omrežij, v zadnjem času pa so na voljo različne možnosti najema pregledovalnika kot storitve, kar omogoča, da podjetja sama periodično pregledujejo svoj informacijski sistem. Glavne značilnosti pregledovalnikov so sledeče:

- iskanje in zaznavanje novih sredstev v informacijskem okolju,
- kategorizacija sredstev,
- zaznavanje ranljivosti,
- zaznavanje skladnosti z regulativami,
- predlaganje varnostnih popravkov in rešitev.

Vsebina zapisov varnostnega pregledovalnika nam dodatno oplemeniti zapise pridobljene iz drugih varnostnih naprav, saj nam pove, ali je neka naprava ranljiva oziroma ali nudimo določeno storitev, ki je ranljiva. Primer zapisa varnostnega pregledovalnika sistemov Nessus Enterprise je predstavljen na sliki 2.6.

62565	CVE-2012-4930		4,3	Medium	server X	tcp	443	Transport Layer Security (TLS) Protocol CRIME Vulnerability	The remote service has a configuration that may make it vulnerable to the CRIME attack.	The remote service has one of two configurations that are known to be required for the CRIME attack : - SSL / TLS compression is enabled. - TLS advertises the SPDY protocol earlier than version 4. Note that Nessus did not attempt to launch the CRIME attack against the remote service.	Disable compression and / or the SPDY service.	http://www.iacr.org/cryptodb/data/paper.php?pubkey=3091 https://discussions.nessus.org/thread/5546 http://www.nessus.org/u?8ec18eb5 https://issues.apache.org/bugzilla/show_bug.cgi?id=53219	The following configuration indicates that the remote service may be vulnerable to the CRIME attack : - SSL / TLS compression is enabled.

Slika 2.6 Primer zapisa zaznane ranljivosti s programsko opremo Nessus Enterprise.

2.2.7 Log spletnega strežnika

V vsakem okolju se srečamo s spletnim strežnikom, ki služi za shranjevanje, izmenjavo in obdelavo informacij ter prikazovanje spletnih strani klientom [5]. Komunikacija med klientom in strežnikom poteka po protokolu za prenos hiperteksta (HTTP) oziroma po njegovi varni različici (HTTPS). Najbolj znani spletni strežniki so IIS, Apache in Nginx. Spletni strežniki so ena od najbolj izpostavljenih storitev v informacijskem okolju, saj praviloma ne omejujemo izvor dostopa do spletnega strežnika, kar pomeni, da je storitev odprta vsem uporabnikom na svetu. Poleg tega veliko spletnih strežnikov, poleg posredovanja podatkov klientom, omogoča tudi sprejem podatkov s strani klientov in izvajanje skript ter poizvedb. Spletne strežnike pogosto najdemo tudi na različnih namenskih napravah kot so stikala, usmerjevalniki, požarne pregrade itd., kjer so uporabljeni kot platforma za dostop do naprave in njeno administracijo.

Primeri zapisov spletnega strežnika vgrajenega v poštni sistem ClearSwift Secure Email Gateway so predstavljeni v zapisu 2.3.

Zapis 2.3 Primeri zapisov spletnega strežnika preko katerega se upravlja s programsko opremo Secure Email Gateway verzije 4.6.0.

```
2017-09-11 22:21:02,610 [0] [AE34FDED32173D0013105A81D9695F0F] [LOGIN] [10.122.1.141] [admin]
2017-09-11 22:21:03,950 [0] [AE34FDED32173D0013105A81D9695F0F] [NAVIGATE] [10.122.1.141] [
    admin] [Home] [/Appliance/HomePage/index.jsp]
2017-09-11 22:21:09,986 [0] [AE34FDED32173D0013105A81D9695F0F] [NAVIGATE] [10.122.1.141] [
    admin] [Logs & Alarms] [/Appliance/SystemsCenter/EventViewer/index.jsp]
2017-09-11 22:23:12,210 [0] [AE34FDED32173D0013105A81D9695F0F] [LOGOUT] [10.122.1.141] [admin]
2017-09-11 22:23:23,707 [0] [109188FAB468D0A4177F2F8BEF0617E9] [LOGINFAILURE] [10.12.11.1] [
    bad.user]
2017-09-11 22:23:27,561 [0] [109188FAB468D0A4177F2F8BEF0617E9] [LOGINFAILURE] [10.12.12.3] [
    bad.user]
2017-09-11 22:23:33,267 [0] [109188FAB468D0A4177F2F8BEF0617E9] [LOGIN] [10.122.1.141] [admin]
2017-09-11 22:23:33,352 [0] [109188FAB468D0A4177F2F8BEF0617E9] [NAVIGATE] [10.122.1.141] [
    admin] [Home] [/Appliance/HomePage/index.jsp]
2017-09-11 22:23:43,403 [0] [109188FAB468D0A4177F2F8BEF0617E9] [NAVIGATE] [10.122.1.141] [
    admin] [Logs & Alarms] [/Appliance/SystemsCenter/EventViewer/index.jsp]
2017-09-11 22:24:05,411 [0] [109188FAB468D0A4177F2F8BEF0617E9] [NAVIGATE] [10.122.1.141] [
    admin] [User Center Home] [/Appliance/UserCenter/index.jsp]
2017-09-11 22:24:42,5 [0] [109188FAB468D0A4177F2F8BEF0617E9] [NAVIGATE] [10.122.1.141] [admin]
     [Modify User] [/Appliance/UserCenter/Modify.jsp?uuid=4783f547-6737-4a53-a7cf-
    d2f58271af2c]
2017-09-11 22:24:44,278 [0] [109188FAB468D0A4177F2F8BEF0617E9] [NAVIGATE] [10.122.1.141] [
    admin] [Apply Configuration Now] [/Appliance/Deployer/DeployNow.jsp]
2017-09-11 22:25:16,557 [0] [109188FAB468D0A4177F2F8BEF0617E9] [LOGOUT] [10.122.1.141] [admin]
```

```
2017-09-11 22:25:24,650 [0] [3ACAEC05A43CCCA6F3170EEA4ED17D14] [LOGIN] [10.122.1.141] [aljosa.
    pocic]
2017-09-11 22:25:24,839 [0] [3ACAEC05A43CCCA6F3170EEA4ED17D14] [NAVIGATE] [10.122.1.141] [
    aljosa.pocic] [Home] [/Appliance/HomePage/index.jsp]
2017-09-11 22:25:26,704 [0] [3ACAEC05A43CCCA6F3170EEA4ED17D14] [NAVIGATE] [10.122.1.141] [
    aljosa.pocic] [User Center Home] [/Appliance/UserCenter/index.jsp]
2017-09-11 22:25:30,953 [0] [3ACAEC05A43CCCA6F3170EEA4ED17D14] [NAVIGATE] [10.122.1.141] [
    aljosa.pocic] [Track Message] [/Appliance/MessageCenter/Tracking/index.jsp]
```

2.3 Spremljanje mrežnega prometa

Dnevniški zapisi običajno ne nudijo dovolj podatkov za popolno analizo dogajanja v informacijskem sistemu, prav tako pa pogosto niso dovolj za dokazovanje dogodkov, ki so se zgodili. Zapisi se praviloma nanašajo na nek dogodek, kot ga je videla varnostna naprava ali operacijski sistem, ne vsebujejo pa forenzičnih podatkov na nivoju paketov, ki bi se lahko uporabili za rekonstrukcijo zaznanega dogodka. Manjkajoče podatke lahko pridobimo s spremljanjem mrežnega prometa.

2.3.1 Zajemanje mrežnega prometa

Zajemanje prometa pomeni prestrezanje podatkovnih paketov, ki prehajajo med različnimi sistemi v omrežju. Ko paket prestrežemo, ga moramo za nadaljnjo obravnavo shraniti. Po zajemu ga lahko z različnimi analizatorji prometa pregledujemo in rekonstruiramo dogodke v omrežju. Zajeti podatki nam omogočajo natančen vpogled v to kaj se je dogajalo na omrežju tako od nivoja komunikacije (kdo s kom in kaj), kot tudi na nivoju podatkov oziroma vpisanih ukazov prenesenih preko omrežja. Najenostavnejši način prestrezanja je uporaba zvezdišč (angl. *hub*), ki posredujejo prejeti signal na vse izhode [6]. Tako moramo na enega od izhodov samo priklopiti napravo, ki omogoča sprejemanje in zajem mrežnega prometa. Že kar nekaj časa nazaj so zvezdišča v informacijskih okoljih v celoti izrinila stikala. Večina stikal omogoča kreiranje tako imenovanega nadzornega porta s pomočjo katerega preusmerimo kopije paketov, ki pridejo na katerikoli port na stikalu na izbrani – nadzorni port. Na slednjega potem priključimo napravo, na kateri spremljamo ali shranjujemo mrežni promet. Slabost te rešitve je, da se lahko v primeru obremenitve stikala na nadzorni port ne kopirajo vsi paketi. Druga bolj zanesljiva možnost je uporaba mrežne prisluškovalne naprave (angl. *network tap*), ki je namenjena izključno temu, da promet, ki prehaja preko nje, kopira tudi na nadzorni port na napravi. Napravo praviloma priključimo na ključna mesta v omrežju kot so povezave do požarnih pregrad in povezave med ključnimi vozlišči. Slabost te rešitve je nezmožnost spremljanja prometa

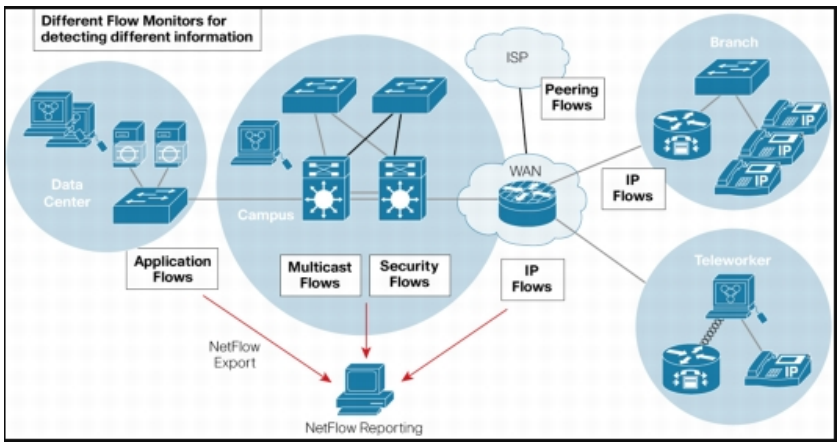
med sistemi priklopljenimi na isto stikalo.
Najbolj znano in najbolj razširjeno brezplačno orodje za pregled in analizo mrežnega prometa je Wireshark [7]. Leta 1997 ga je začel razvijati Gerald Combs, ki je potreboval orodje za sledenje mrežnim problemom in orodje, ki bi mu pomagalo pri učenju o omrežjih. Tako je julija 1998 izšla prva verzija orodja Ethereal, ki se je razvijal in leta 2006 preimenoval v Wireshark.
Zajem prometa se lahko izvaja tudi na delovnih postajah, strežnikih in požarnih pregradah, vendar pa je slednje koristno samo v primeru potrebe po dodatnem dokazovanju aktivnosti, ki jo je z beleženjem zaznal sistem.

2.3.2 NetFlow

NetFlow je omrežni protokol razvit s strani podjetja Cisco [8] z namenom spremljanja, analize in nadzora omrežnega prometa. Z analizo spremljanega prometa lahko pridobimo informacijo o tokovih in količini omrežnega prometa. Tako dobimo informacije o uporabljenih protokolih in aplikacijah ter vpogled v to, kateri sistemi komunicirajo med seboj in kje v omrežju prihaja do zakasnitev. Spremljanje NetFlow-a nam omogoči delno rekonstrukcijo dogodka, ki se je zgodil v našem okolju. Tipična arhitektura sistema je sestavljena iz naprave, ki generira NetFlow zapise (stikalo, usmerjevalnik, požarna pregrada) iz naprave, ki zbira te zapise imenovane NetFlow Collector in konzole iz katere se izvaja analiza zbranih zapisov. Primer postavitve arhitekture in zajema podatkov z NetFlow protokolom je prikazan na sliki 2.7. Kljub dejstvu, da je bil protokol razvit s strani podjetja Cisco, ga poleg njih na svoji opremi danes podpira večina vodilnih proizvajalcev mrežne opreme kot so Juniper, Aruba (HP), Nortel itd. Nekateri proizvajalci uporabljajo tudi svoje protokole kontrole pretoka kot so JFlow (Juniper), S-Flow (HP) itd. Z namenom poenotenja spremljanja, analize in nadzora omrežnega prometa se je na osnovi NetFlow protokola razvil Internet Protocol Flow Information Export (IPFIX) protokol [9]. IPFIX protokol določa način in format prenosa informacije o prometnih tokovih preko omrežja.

2.4 Načini za preverjanje virov informacij

Informacijsko okolje mora biti tesno povezano in v podporo poslovnim procesom. Omogočati mora hitre prilagoditve informacijskih rešitev na nove poslovne razmere, hkrati pa mora zagotavljati visok nivo varnosti uporabe informacijskih storitev. Pogosto je komunika-



Slika 2.7 Prikaz postavitve NetFlow zajema podatkov [10].

cija s poslovnimi partnerji iz vidika varnosti obravnavana drugače kot komunikacija z ostalimi. Varnostno tveganje v takšnem primeru je v tem, da pogosto nimamo možnosti nadzirati varnostnih mehanizmov, ki jih uporabljajo poslovni partnerji. Posledično svoje informacijsko okolje izpostavimo varnostnemu tveganju informacijskega okolja poslovnega partnerja. Kot primer lahko navedemo nastavitev izjeme za varnostna preverjanja partnerjeve domene pri pregledovanju elektronske pošte. Razlog je lahko v preteklosti zaustavljena elektronska pošta poslana s strani partnerja, ki ni bila skladna z varnostnimi nastavitvami našega sistema zaradi napačnih ali nepopolnih nastavitev poštnega strežnika na strani pošiljatelja. Ker je poslovna potreba prevladala nad varnostno zahtevo, se je naredila izjema v politiki preverjanja. Prav tako se je veliko vsebine in komunikacije preselilo v elektronsko obliko in tako uporabniki prejemajo vsebine iz različnih elektronskih virov. Pogosto so ti viri za njih novi in jim ne zaupajo. Z izobraževanjem uporabnikov so le ti postali bolj pozorni na prejeto vsebino oziroma na vir, ki jim posreduje to vsebino.

Skrbnik za varnost v informacijskem sistemu se tako srečuje z dvema vrstama vprašanj:

- ali je vsebina iz neznanega vira res nevarna,
- ali je vsebina iz znanega vira res varna.

Kljub temu, da se vsebina praviloma pregleduje z različnimi varnostnimi mehanizmi, pa nobena zaščita ne more zagotoviti popolne informacijske varnosti in pravilnosti zaznave brez lažno pozitivnih rezultatov. Na svetovnem spletu so na voljo različne strani, ki

ponujajo orodja, s katerimi lahko pridobimo različne informacije o viru vsebine, ki jo želimo prejeti iz svetovnega spleta oziroma s katerimi lahko preverimo varnost prejetih datotek.

2.4.1 Orodja za ugotavljanje izvora vsebine

Poznavanje izvora vsebine nam lahko pomaga pri odločitvi o tem ali dovolimo dostop do neke datoteke ali ne. Izvor sam po sebi ni zagotovilo za popolno varnost, vendar pa lahko občutno zmanjša varnostna tveganja v informacijskem okolju. Kot primer bi lahko navedli okolje, v katerem ne dovolimo prenos izvršljivih datotek iz svetovnega spleta. Pri tem je dovoljena izjema, ki dovoljuje prenos takšnih datotek iz domene *.microsoft.com. Prenos izvršljivih datotek iz te domene je namreč nujen za posodobitve Microsoft Windows operacijskega sistema.

Svetovni splet nam nudi množico praviloma brezplačnih orodij s katerimi lahko preverimo zgodovino in ugled IP naslova ali domene. Tako lahko preverimo:

- lastnika domene,
- starost domene,
- DNS nastavitve za domeno,
- lokacijo na kateri se nahaja nek strežnik,
- kategorizacijo spletne strani,
- varnost spletne strani,
- izkušnje uporabnikov pri dostopu do spletne strani,
- zgodovino strani (posnetek strani preko več let),
- nastavitve povezane z elektronsko pošto, ki nam povedo, kdo lahko pošilja pošto za določeno domeno (SPF),
- nastavitve poštnega strežnika, kot so podpora TLS, pozdravno okno,
- uvrščenost strežnika na RBL liste,
- oceno količine posredovane elektronske pošte,
- pot preko omrežij do ciljnega naslova iz različnih virov.

Na osnovi tako pridobljenih podatkov se lažje odločimo ali lahko zaupamo nekemu viru, ali pa so potrebna dodatna varnostna preverjanja vsebine. Primer spletne strani, ki nam omogoča pridobitev informacij o IP naslovu, domeni ali lastniku omrežja, je Talos v lasti podjetja Cisco [11].

2.4.2 Orodja za varnostno analizo datotek

Navkljub implementiranim varnostnim rešitvam v informacijskem okolju se lahko pojavi dvom o varnosti datoteke ali spletne strani. Določen promet se namreč na komunikacijski poti ne more pregledovati, na končni točki pa imamo praviloma nameščeno samo eno varnostno zaščito. Obstaja veliko orodij, ki omogočajo dodatno varnostno analizo datotek. Ta orodja so lahko nameščena v informacijskem okolju samem in jim preko različnih protokolov (CIFS, SCP, ipd.) posredujemo sumljivo datoteko v pregledovanje. Primer takšnega produkta je na primer File Content Security rešitev proizvajalca FireEye [12]. Nekatera orodja so na voljo tudi na svetovnem spletu in ne zahtevajo namestitve v lokalnem okolju. Prednosti teh orodij sta cena in hitrost vpeljave rešitve v informacijsko okolje, lahko pa se pojavi pomislek o posredovanju datotek s poslovno vsebino ali osebnimi podatki v svetovni splet. Najbolj znana spletna stran takšne vrste je spletna stran virustotal [13], ki omogoča pregledovanje datotek in spletnih naslovov z okrog 60 različnimi anti virusnimi programi. Stran je koristna predvsem pri zaznavanju znanih okužb, za katere obstaja poznan vzorec obnašanja ali kontrolni seštevek. Za simulacijo dogajanja na sistemu po odprtju datoteke oziroma za iskanje še nezananih napadov je na voljo stran Payload Security [14], ki uporablja VxStream Sandbox rešitev za izvajanje analize.

3 Zbiranje, pregledovanje in koreliranje zapisov

3.1 Uvod

Kot smo videli v prejšnjem poglavju, se v informacijskem okolju srečamo z množico zelo različnih tipov dnevniških zapisov. Zapisi se lahko nahajajo lokalno na sistemu ali pa se posredujejo na oddaljeni sistem. Praviloma skrbniki posameznih sistemov pregledujejo lokalno shranjene zapise in preverjajo ali se na sistemu dogaja nekaj, kar ni v skladu s pričakovanji. Težava pri tem je, da sta lahko skrbnik sistema in aplikacije različni osebi in gledata vsaka svoj zapis ter tako pridobita samo delne informacije o stanju sistema. Težava je tudi v tem, da se lahko generira velika količina zapisov na sistemu in jih je nemogoče pregledati brez posebnih orodij. Tretja težava je v tem, da s pregledovanjem samo lokalnih dnevniških zapisov pogosto nimamo vseh potrebnih informacij za zaznavo usmerjenih in kompleksnih napadov, da pogosto ne moremo ugotoviti izvora napada in kdo vse je še udeležen v njem, oziroma kakšne so posledice nekega varnostnega dogodka. Prav tako so lokalno shranjeni zapisi lahko podvrženi spreminjanju ali brisanju, s čimer lahko napadalec zakrije svoje sledi. Težava je lahko tudi potreben prostor za shranjevanje zapisov sistema še posebno za daljše obdobje.

3.2 Zgodovina SIEM sistemov

V zgodovini so se pojavili sistemi za lokalno spremljanje zapisov, ki so zmanjšali tveganje spremembe dnevniških datotek s strani napadalca in olajšali delo skrbniku sistema pri pregledovanju zapisov na sistemu. Sistem je delal tako, da je periodično pregledoval definirane dnevniške datoteke in v njih bodisi iskal zapise, ki so ustrezali nekemu vzorcu ter jih javljal skrbniku, bodisi javljal vsak neizločen zapis, ki se je pojavil v dnevniški datoteki. Eden najbolj znanih sistemov te vrste je bil Logsentry [15]. Kasneje so se pojavili sistemi za centralizirano sprejemanje in shranjevanje dnevniških zapisov, ki so se tekom let razvili v SIEM sisteme. SIEM je kratica za angleško besedo Security Information and Event Management. V literaturi se pojavljajo tudi kratice SEM (angl. *Security Event Management*) in SIM (angl. *Security Information Management*). SIEM nam daje celovit, enoten pogled tako na infrastrukturo in storitve v našem okolju, kot tudi na skladnost poteka dela s pravilniki in regulativami. Omogoča nam centralno upravljanje z dnevniškimi zapisi in zagotavlja dokaze o zaznanih dogodkih [16]. Prvi SIEM sistemi so se začeli pojavljati okrog leta 2000 z namenom centralnega zbiranja zapisov iz varnostnih naprav, predvsem zgodnjih sistemov za detekcijo vdorov (angl. *intrusion detection systems*), ki so generirali velike količine zapisov [17]. Omogočali so zaznavo enostavih soodvisnosti. Naj jih nekaj naštejemo:

- če vidiš poizkus izkoriščanja ranljivosti sistema A z namenom pridobitve oddaljenega dostopa in
- vidiš oddaljeni dostop iz sistema A do sistema B potem
- pošlji obvestilo skrbnikom sistema A in B.

Sistemi niso imeli vključenih nobenih ali zelo malo normalizacij dnevniških zapisov in vgrajenih korelacij med različnimi zapisi ter so zahtevali tako poznavanje informacijskega okolja, kot tudi ogromno znanj iz različnih področij.

Prvi SIEM sistemi so bili tako centralno mesto za shranjevanje različnih zapisov. Nudili so enoten vmesnik za iskanje enostavnih soodvisnosti ter preverjanje skladnosti in varnosti informacijskega sistema. Omogočali so tudi postavljanje različnih prioritet zaznanih dogodkov in alarmiranje. V nadaljevanju je osnovni namen SIEM rešitev varnosti prevzela potreba po skladnosti (npr. PCI-DSS regulativa) in SIEM sistemi so bolj

kot varnostna rešitev postali sistem za analizo log zapisov. Paralelno so se pojavile zahteve po poglobljeni analizi dogajanja pred, med in po napadu ali okužbi informacijskega sistema. Za takšno analizo prvi SIEM sistemi niso bili narejeni, imeli pa so podatke v bazah, zato so si analitiki pomagali z njimi. Pokazale so se omejitve uporabljenih relacijskih baz in potrebe po analitični platformi, ki bi bila prilagojena velikim količinam podatkov in bi omogočala hitro iskanje kompleksnih soodvisnosti. V letih 2010 do 2011 so se na trgu zgodili večji prevzemi takrat vodilnih ponudnikov SIEM sistemov in sicer je podjetje Hewlett-Packard prevzelo podjetje ArcSight, IBM je prevzel Q1 Labs in McAfee je prevzel Nitro Security. Namen teh podjetij je bil postaviti SIEM rešitve v središče informacijske varnosti kot točko, v kateri se združijo vse varnostne rešitve.

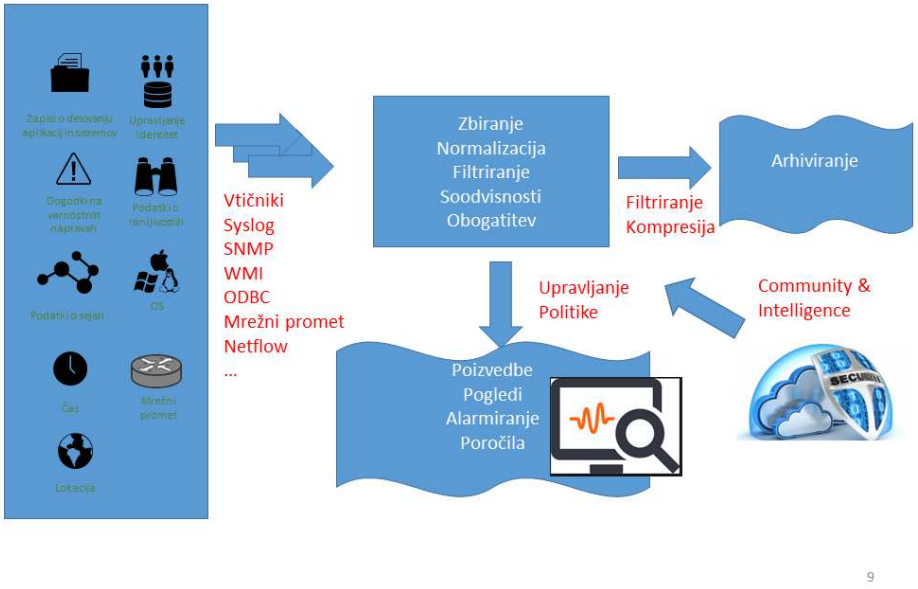
3.3 Napreden SIEM sistem

Iz sistema za centralizirano shranjevanje zapisov in doseganje skladnosti je SIEM postal glavno varnostno orodje v informacijskem okolju. Zaradi velike količine zapisov in potrebe po spremljanju mrežnega prometa se uporabi namenska platforma za velike podatke (angl. *big data*), ki omogoči zbiranje velike količine različnih tipov podatkov, fleksibilnost in hitro obdelavo ter iskanje soodvisnosti. Preko enotnega vmesnika se različni tipi uporabnikov prijavljajo v sistem, kjer so pogledi prilagojeni njihovim vlogam in iz katerega lahko izvajajo vse njihove aktivnosti na SIEM sistemu. Tako so funkcionalnosti, ki jih pričakujemo od naprednega SIEM sistema, naslednje:

- zbiranje zapisov, dogodkov in mrežnega prometa,
- normalizacija in razčlenjevanje podatkov,
- iskanje soodvisnosti,
- obogatitev podatkov,
- večnivojski pogledi in vrtanje v globino,
- kreiranje poročil in alarmiranje,
- arhiviranje podatkov.

Komponente in funkcionalnosti SIEM sistema nam prikazuje slika 3.1.

SIEM sam po sebi nima mehanizma za preprečevanje okužb, blokiranje napada ali izolacijo okuženega sistema, pomaga pa nam zmanjšati tako imenovani “DWELL time”

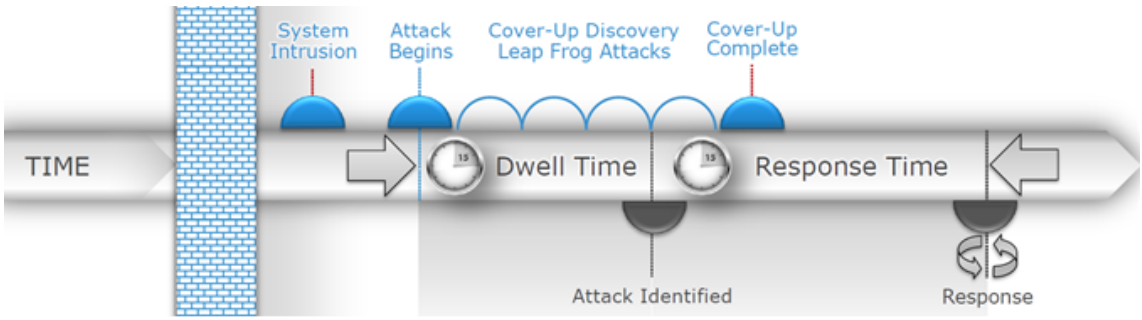


Slika 3.1 Komponente in funkcionalnosti naprednega SIEM sistema.

[18], to je čas, ki mine od okužbe vira v informacijskem sistemu do odkritja te okužbe, kot je prikazano na sliki 3.2. Pogosto se zgodi, da podjetja potrebujejo tudi po več tednov ali mesecev, preden ugotovijo okužbo v svojem informacijskem sistemu. Tako je recimo podjetje Yahoo! šele v drugi polovici leta 2016 odkrilo krajo podatkov o 500 milijonih uporabnikov, ki se je zgodila konec leta 2014 [19]. S skrajšanjem časa, ki mine med okužbo in zaznavo, omejimo odtekanje informacij iz okolja in zmanjšamo možnost okužbe drugih sistemov znotraj okolja.

3.3.1 Zbiranje zapisov, dogodkov in mrežnega prometa

Zapisi in dogodki pridobljeni iz različnih virov ter mrežni promet so osnova za vse nadaljnje aktivnosti. Pomagajo nam razumeti kdo nas danes napada in tudi kako se je zgodil nek varnostni incident, kako je prišel v naše okolje, kaj je povzročil in kdo vse je okužen. Količina in kvaliteta prejetih podatkov so bistveni za kvaliteto analiz in poročil, ki jih izvajamo. Zato je zelo pomembno, da pridobimo zapise iz vseh naprav in storitev, ki se nahajajo v informacijskem okolju. Tukaj je pomembno, da zajamemo tudi naprave, ki niso običajni del IT sistemov, kot so na primer registratorji časa, alarmni sistemi, kamere,



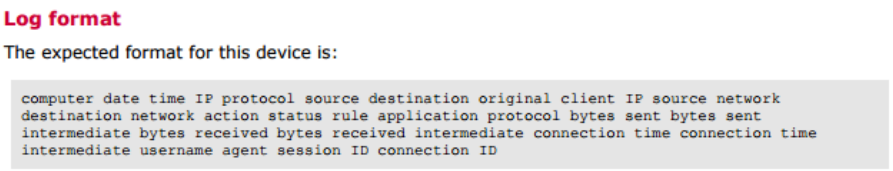
Slika 3.2 Prikaz časa med okužbo in zaznavo [20].

telefoni ipd. Samo zbiranje zapisov se lahko izvaja na tri različne načine [21]:

- preko agentov, ki se namestijo na končne sisteme,
- s pošiljanjem zapisov iz končnih točk in mrežnih naprav na komponento SIEM sistema zadolženo za zbiranje podatkov,
- preko povezave iz komponente SIEM sistema za zbiranje podatkov do končnih sistemov.

Že v fazi zbiranja zapisov je potrebno zapisom dodati časovno komponento centralnega sistema (angl. *timestamp*) in določene zapise filtrirati ter izločiti iz shanjevanja. Praviloma gre za zapise informativne narave, ki nimajo dodane vrednosti za razumevanje stanja v informacijskem sistemu, se pa pojavljajo v velikih količinah.

Uporaba agentov na končnih sistemih prinese določene prednosti, kot sta možnost izvajanja naprednega filtriranja dogodkov na izvoru zapisov in pošiljanje zapisov na SIEM v realnem času, kar zmanjša možnost manipulacije z njimi [22]. Ni pa primerna za vsak tip naprav (npr. namenske naprave, mrežno opremo), prav tako pa prinese tveganje kompatibilnosti dodatne programske opreme na sistem. Danes sta tako veliko bolj razširjena druga dva načina. Končne točke tako v realnem času pošiljajo zapise na SIEM sistem. Običajno se za takšno posredovanje uporabita SNMP ali "syslog protokol". Pri uporabi "syslog" protokola je potrebno biti pozoren na to, da poteka komunikacija preko šifriranega kanala. Pri SNMP protokolu se priporoča uporaba verzije 3, ki omogoča avtentikacijo in šifriranje pri prenosu zapisov. Tudi pri tem načinu se zagotovi pošiljanje zapisov v realnem času, potrebno pa je upoštevati, da uporaba šifriranih povezav zahteva



Slika 3.3 Primer preslikave zapisa požarne pregrade Check Point na McAfee ESM [21].

nekaj procesorske moči tudi na strani pošiljatelja. Pri tretjem načinu omogočimo komponenti SIEM sistema zadolženi za zbiranje zapisov, da se poveže na vir zapisov preko določenega protokola. Primer takšne povezave je povezovanje na SQL strežnik preko ODBC povezave. Prednost tega načina je na primer možnost izbire frekvence povezovanja na vir dogodkov in hkratni prenos večih zapisov, kar je performančno manj zahtevno kot prenašanje posameznega zapis. Slabost je ta, da obstaja možnost spremembe zapisa na viru, še predno se zapis prenese na SIEM sistem.

3.3.2 Normalizacija in razčlenjevanje

V tej fazi se zapisi pretvorijo na skupni imenovalec. Posamezen zapis je potrebno razdeliti na polja, ki jih lahko potem uporabimo pri iskanju soodvisnosti. Da lahko to naredimo, moramo poznati strukturo zapisa vira. Zaradi velikega števila različnih virov je zelo pomembno, da že proizvajalec SIEM sistema v svoji rešitvi ponuja razčlenjevalnike strukture zapisov za kar največ različnih virov. Skrbnik SIEM sistema mora tako za posameznen vir samo navesti tip (npr. CheckPoint požarna pregrada verzije R80.10) in sistem potem uporabi ustrezen razčlenjevalnik. Za nestandarne aplikacije mora SIEM sistem omogočati uporabo individualnih razčlenjevalnikov, ki jih skrbnik SIEM sistema razvije skupaj z razvijalcem aplikacije. Primer oblike zapisa požarne pregrade Check Point kot ga pričakuje McAfee SIEM sistem, je predstavljen na sliki 3.3.

3.3.3 Obogatitev podatkov

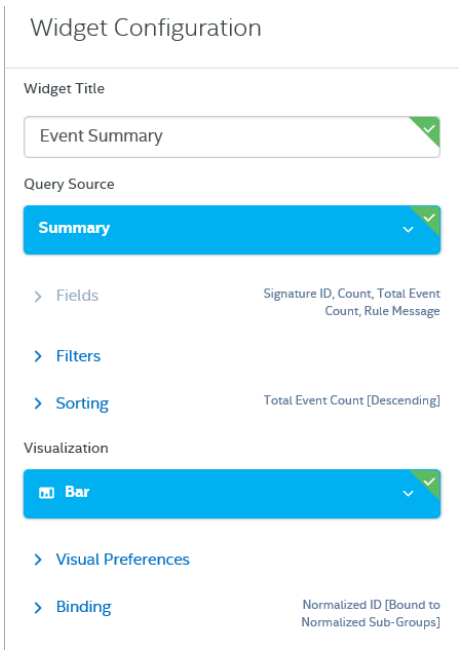
Zapisi vsebujejo podatke, kot jih vidijo sistemi, ki jih posredujejo. Sistem za preverjanje elektronske pošte tako vidi pošiljanje kriptirane elektronske pošte med pošiljateljem in prejemnikom. Ne razlikuje ali gre za izmenjavo podatkov med dvema poslovnima partnerjema, ali pa je takšna pošta prišla od neznanega pošiljatelja iz strežnika na Kitajskem do vodje računovodstva. V prvem primeru gre lahko za del poslovnega procesa, medtem ko je v drugem primeru smiselno preveriti, ali je prejemnik po prejemu elek-

tronske pošte izvedel kakšne nenavadne akcije. Podatkom je smiselno dodati vsebino, ki nam lahko pomaga zaznan dogodek postaviti v poslovni kontekst. Tipično se dodajajo sledeče vsebine:

- geografska lokacija,
- skrbnik sistema in kontaktni podatki,
- kritičnost sistema,
- položaj posameznika v organizaciji,
- podatki o ranljivostih sistema,
- podatki iz svetovnega spleta.

3.3.4 Iskanje soodvisnosti

Iskanje soodvisnosti je bistvo SIEM sistema. Pri njem gre za pisanje pravil, s katerimi iz zapisov različnih naprav zaznamo kompleksne varnostne incidente ali anomalije pri obnašanju uporabnikov. Da lahko povežemo različne zapise, jih moramo v fazi razčlenjevanja pravilno razčleniti in tako zagotoviti pravilno povezovanje. Primer iskanja kompleksne soodvisnosti je na primer povezovanje zaznanega dogodka IPS sistema z rezulati pregledovalnika sistemov in ugotovitev ali zaznani dogodek pomeni varnostno tveganje. Da skrbnik SIEM sistema pravilno zapiše pravila, je poleg poznavanja SIEM sistema potrebno dobro poznavanje informacijskega okolja in visok nivo znanja iz varnosti informacijskih sistemov. Primer je lahko pravilo, ki povezuje zapise iz aktivnih imenikov podjetja v različnih državah. Na prvi pogled je v primeru, da se isti uporabnik v kratkem časovnem razmiku prijavi na sisteme v dveh ali več aktivnih imenikov, potrebno generirati alarm, vendar pa lahko obstajajo določeni domenski uporabniki s specifičnimi vlogami za katere je takšno obnašanje pričakovano. Kot primer lahko navedemo pregledovalnik sistemov, ki uporablja enega domenskega uporabnika za sisteme v podjetju iz različnih držav. Ob zagonu pregledovanja se ta sistem prijavi na različne sisteme v kratkem časovnem obdobju. Pri pisanju soodvisnosti je potrebno paziti na njihovo strukturo, saj slabo napisane soodvisnosti ne dajo pravih rezultatov in tudi močno obremenijo sistem.



Slika 3.4 Primer izgradnje gradnika.

3.3.5 Večnivojski pogledi in vrtanje v globino

Če želimo, da SIEM sistem prevzame centralno vlogo v varnosti informacijskega sistema, moramo zagotoviti, da ima posamezen uporabnik na voljo prave podatke. SIEM sistem je namenjen uporabnikom z različnimi vlogami v informacijskem sistemu. Še posebej v večjih organizacijah se lahko pravice in dolžnosti uporabnikov poleg različnih vlog (npr. vodja razvoja, vodja marketinga) omejujejo tudi na geografske kriterije (npr. država ali regija). Zaradi velikega števila virov, ki se vklopijo v SIEM sistem, imajo uporabniki na voljo ogromno dogodkov in ni vedno potrebno, da vsi uporabniki vidijo vse vire in dogodke. Tako je pomembno, da lahko prilagodimo izgled nadzorne plošče vlogi posameznega uporabnika. Izgradnja pogleda se izvaja s pomočjo gradnikov pogleda, ki jih dodajamo posameznemu pogledu. Posameznemu gradniku moramo določiti ime, tip poizvedbe (angl. *query*) in tip vizualizacije, kot je razvidno iz slike 3.4. Tako začnemo nadzorno ploščo za glavnega varnostnega inženirja graditi s splošnim pregledom celotnega okolja, ki vsebuje agregirane podatke kot je število dogodkov in njihova distribucija skozi čas, glavni izvori in cilji ter uporabniki [23]. Potem ji dodamo še poglede kot so število posameznih dogodkov, glavni viri in aplikacije. Nadzorno ploščo za analitika začnemo graditi z zaznanimi dogodki sortiranimi po kritičnosti. Sistem mora tudi omogočati eno-

stavno vrtanje v globino (angl. *drill-down*). Uporabnik klikne na podatek, ki ga zanima (na primer IP naslov izvora dogodka) in v nadzorni plošči se avtomatično posodobi prikaz dogodkov, ki so filtrirani glede na izbrani podatek. Tako na primer pregled najbolj pogostih dogodkov, sedaj prikazuje najbolj pogoste dogodke, katerih izvor je izbrani IP naslov. Nadzorna plošča mora omogočati tako spremljanje stanje v informacijskem okolju v realnem času, kot tudi vpogled na stanje v izbranem preteklem časovnem obdobju.

3.3.6 Kreiranje poročil in alarmiranje

Namen poročil je enostavno pridobiti hiter pogled v dogajanje za izbrano preteklo obdobje. Preko poročil lahko spremljamo trende z varnostjo povezanih dogodkov skozi čas. Služijo nam lahko kot osnova pri revizorskih pregledih zunanjih poslovnih partnerjev ali regulatorjev. Napredni SIEM sistemi imajo tako že vgrajena predpripravljena poročila iz različnih kategorij, ki jih lahko prilagodimo našim zahtevam. Najbolj tipična poročila so:

- vodstveni pogled,
- pregled ranljivosti,
- pregled tveganj,
- pregled dogodkov,
- pregled komunikacijskih tokov,
- skladnost z regulativami (PCI, HIPAA, 27002, itd.).

V primeru, da SIEM sistem zazna kritičen varnostni dogodek, je zaželjeno, da ima vgrajen sistem obveščanja ali alarmiranja. Ker v SIEM sistem v fazi obogatitve podatkov lahko pripeljemo informacije o skrbnikih sistemov in organizacijsko strukturo, lahko v SIEM sistemu dokaj enostavno določimo koga je potrebno obvestiti ob zaznanem dogodku ali alarmirati v primeru zlonamernega obnašanja zaposlenega. Funkcionalnost alarmiranja nam omogoča, da SIEM sistem povežemo s sistemom za obravnavo incidentov. Nekateri SIEM sistemi imajo tudi že sami vgrajen osnovni sistem za obravnavo incidentov.

3.3.7 Arhiviranje podatkov

Za analizo trenutnega stanja varnosti informacijskega sistema potrebujemo podatke za krajše časovno obdobje tja do treh mesecev. Včasih je potrebno določene podatke hraniti zaradi zakonskih zahtev ali pa tudi morebitnih poslovnih potreb po naknadnem dokazovanju ali analizi dogodkov. Podatke je potrebno shraniti na način, da so še vedno dostopni za izvajanje poročil in analizo. Zaradi velike količine podatkov je pri arhiviranju potrebno zagotoviti kompresijo podatkov in tudi filtriranje podatkov, ki jih shranjujemo za daljše obdobje. Filtriranje pomeni, da se določenim podatkom odrečemo in jih ne shranjujemo. Tukaj se moramo odločiti za podatke, ki so samo informativnega pomena, ali pa se odločimo, da za daljše obdobje ne shranjujemo celotnega mrežnega prometa, temveč samo podatke o vzpostavljenih sejah. Pri kompresiji podatkov se je potrebno zavedati, da večja kompresija sicer pomeni, da lahko shranimo več podatkov, vendar pa traja dalj časa, da so arhivirani podatki ponovno dostopni za analizo.

4 Implementacija SIEM sistema v vzorčnem informacijskem okolju

4.1 Uvod

V pričujočem poglavju opišemo primer implementacije SIEM rešitve v vzorčnem informacijskem okolju. Predstavimo uporabljeno SIEM rešitev, gradnike vzorčnega informacijskega okolja in integracijo posameznega vira vanjo. Na nekaj primerih pokažemo načine izgradnje avtomatičnega iskanja soodvisnosti med različnimi dogodki ter načine pregledovanja zapisov iz SIEM sistema. Pokažemo prilagojene poglede za različne tipe uporabnikov SIEM sistema in primer izvedbe dodatne analize zaznane škodljive kode.

4.2 Opis naročnika

Naročnik je večje trgovsko podjetje prisotno v Sloveniji, Srbiji, Črni Gori, Bosni in Hercegovini in na Hrvaškem. V Sloveniji se nahajajo sedež podjetja, oddaljene lokacije in tudi podatkovni center. V ostalih državah se nahajajo centralna lokacija in oddaljene lokacije. Oddaljene lokacije so lahko trgovine, skladišča ali mobilne trgovine, na centralni lokaciji pa se nahajajo skupne službe in vodstveni kader posamezne države. Skupno število oddaljenih lokacij presega številko 120, skupno število zaposlenih pa se giblje okrog tisoč.

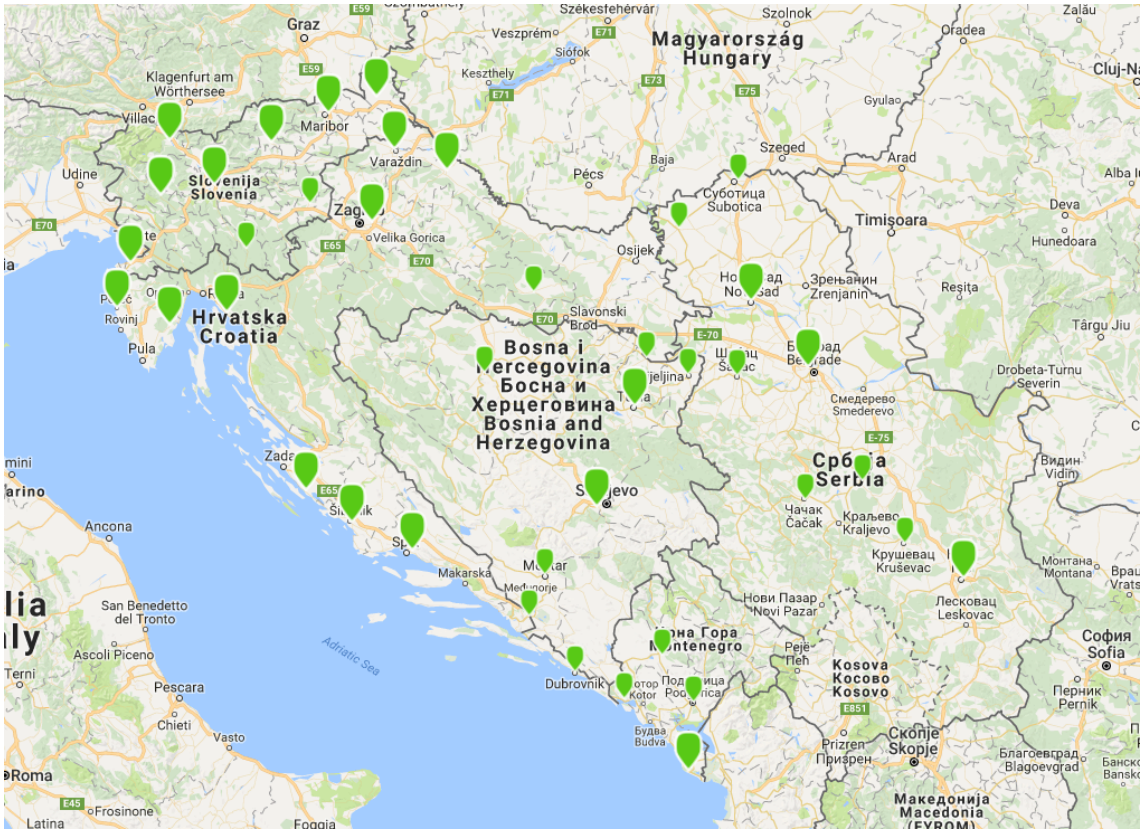
Poleg klasičnih trgovin podjetje nudi tudi spletno trgovino, ki je namenjena kupcem iz jugovzhodne Evrope. Podjetje razpolaga z različnimi podatki, ki so podvrženi regulativam varovanja podatkov in tudi s podatki, ki so kritični za poslovanje. Te vrste podatkov so:

- podatki o kupcih,
- podatki o dobaviteljih,
- podatki o zunanjih partnerjih,
- podatki o zaposlenih,
- nabavne cene.

V borbi za kupce podjetje veliko pozornosti posveča ugledu, ki ga dosega na trgih, kjer je prisotno. Za podjetje sta zelo pomembni tudi hitrost in prilagodljivost. Tako mora biti podjetje sposobno v enem dnevu prestaviti mobilno trgovino na drugo lokacijo in naslednji dan nemoteno obratovati, kar pomeni dosegljivost vseh storitev iz podatkovnega centra in dostop do interneta. Dosegljivost mora biti omogočena ne glede na ponudnika in tip povezave (optika, xDSL, mobilni dostop) do interneta, ki jo ima mobilna trgovina na novi lokaciji. V primeru izjemnih vremenskih pojavov (vročina, mraz, sneg, itd.) podjetje hitro reagira in potrošniku ponudi primeren izdelek. Na primer v hudi vročini ponudi pijače in izdelke za na plažo, v primeru snežnih metežev pa v trgovinah na tem področju ponudi naprave in orodja za odstranjevanje snega. Informacijski sistem v podjetju mora tako omogočati dovolj veliko fleksibilnost in hkrati enostavnost, ki omogočita hitro prilagajanje na različne poslovne potrebe. Hkrati pa je zelo pomemben vidik varnosti, ki poleg varovanja občutljivih podatkov varuje tudi ugled podjetja. Slika 4.1 nam prikazuje lokacije naročnika v celotni regiji.

4.3 Opis vzorčnega okolja

Centralno mesto v vzorčnem okolju ima podatkovni center, ki je najet pri zunanjemu ponudniku. V podatkovnem centru tečejo vse poslovne in podporne aplikacije, potrebne za delovanje naročnika. V njem se nahajajo spletni in poštni strežniki ter strežniki namenjeni shranjevanju podatkov. Podatkovni center se nahaja na dveh lokacijah, ki sta med seboj povezani z dvema neodvisnima najetima povezavama prepustnosti 10Gbps. Povezavi tečeta po različnih trasah, kar zagotavlja redundantnost v primeru fizičnih poškodb



Slika 4.1 Lokacije naročnikovih trgovin in central.

linij. Logično sta povezavi narejeni na nivoju povezovalne plasti OSI modela [24], kar zagotavlja enostavno selitev strežnikov iz ene na drugo lokacijo. Preko ene fizične povezave je speljanih več virtualnih omrežij (angl. *Virtual Lan* (VLAN)) [25], ki se zaključujejo na stikalih v podatkovnem centru. Preko usmerjanja na teh stikalih je odvisno, ali poteka komunikacija med dvema strežnikoma direktno, ali preko požarne pregrade. Na posamezni lokaciji se nahajata dva virtulizacijska sistema, ki gostita virtualne strežnike. Virtualizacijski sistem je narejen tako, da se v primeru izpada sistema na eni lokaciji aktivira redundanten sistem na drugi, ki gosti iste virtualne strežnike.

Podatkovni center ima tudi popolnoma podvojeno povezavo do interneta, kar pomeni dve neodvisni fizični povezavi, dva usmerjevalnika, ki preko BGP protokola oglašujeta neodvisni naslovni prostor naročnika v internet in podvojeno požarno pregrado. Po en sistem usmerjevalnika in požarne pregrade se fizično nahaja na posamezni lokaciji. Shema podatkovnega centra je prikazana na sliki 4.2.

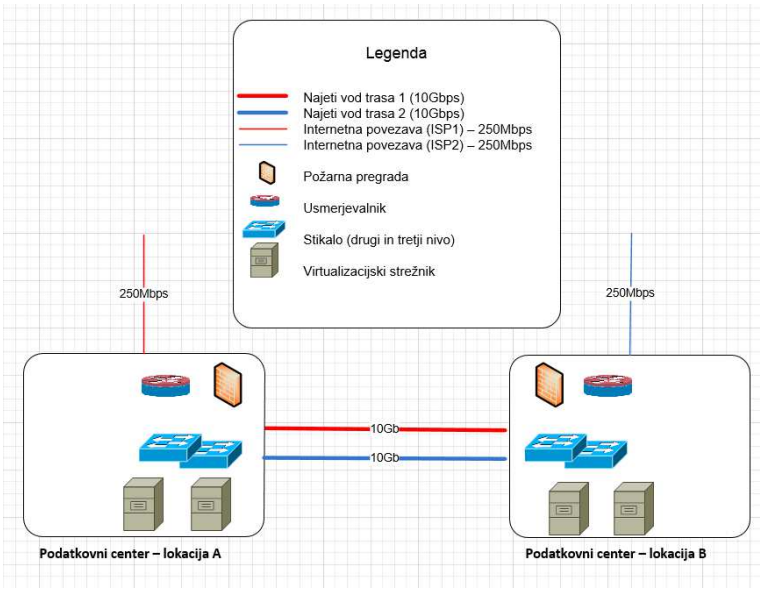
V vsaki državi obstaja ena centralna in več oddaljenih lokacij. Oddaljene lokacije so preko kriptirane povezave povezane v centralno lokacijo v isti državi. Vsa komunikacija iz oddaljene lokacije do podatkovnega centra, ostalih lokacij in interneta poteka preko centralne lokacije v isti državi. Centralna lokacija ima vzpostavljeno kriptirano povezavo do podatkovnega centra in lokalni dostop do interneta. Na oddaljeni lokaciji se nahaja naslednja vrsta opreme: prenosnik, delovna postaja, mrežno stikalo, dostopna točka, požarna pregrada in alarmna naprava. Vrsta opreme na centralnih lokacijah je enaka z razliko požarne pregrade, ki je podvojena in opravlja storitve požarne pregrade naslednje generacije (angl. *Next Generation Firewall*) in virtualiziranega strežnika z Microsoft Windows operacijskim sistemom. Shema poteka komunikacij v vzorčnem okolju je prikazana na sliki 4.3.

4.4 Vrste naprav v informacijskem okolju naročnika

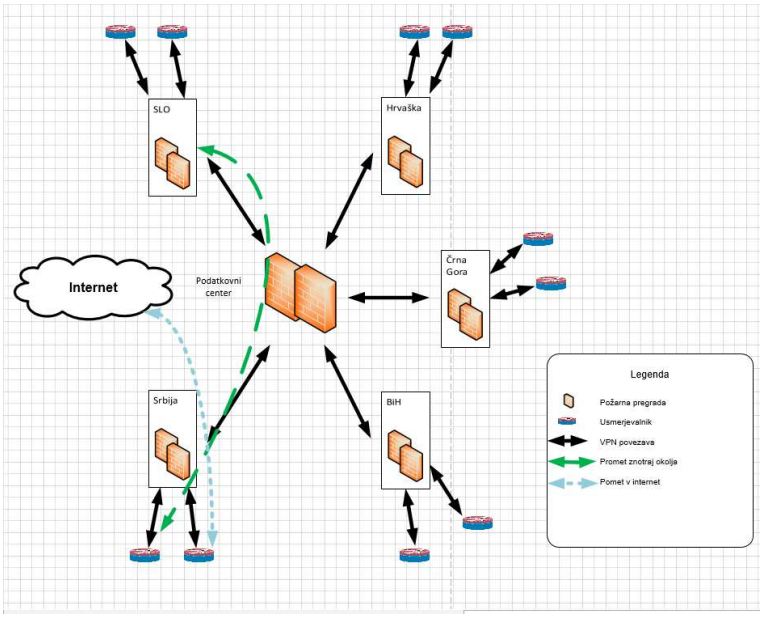
Poglavje podrobneje opisuje naprave in sisteme uporabljene v vzorčnem okolju. Navedena je verzija uporabljene programske opreme ali operacijskega sistema, namen uporabe in kritičnost sistema iz vidika informacijske varnosti.

4.4.1 Strežniki

V vzorčnem okolju se na strežnikih uporabljata tako Windows, kot tudi Linux operacijski sistem. Del Windows strežnikov je že bil nadgrajen na verzijo Server 2012 R2, medtem ko



Slika 4.2 Shema okolja podatkovnega centra na dveh lokacijah.



Slika 4.3 Prikaz poteka komunikacij med dvema lokacijama in v internet.

drugi del še vedno uporablja operacijski sistem Server 2008 R2. Strežniki z nameščenim Linux operacijskim sistemom imajo nameščeno verzijo CentOS-7. Na strežnikih tečejo poslovne in infrastrukturne aplikacije ter podatkovne zbirke. Windows strežniki so člani domene in omogočajo prijavo z domenskim geslom, Linux strežniki pa niso člani domene, dostop do strežnikov je omogočen preko dvo faktorske avtentikacije. Na strežnikih tečejo aplikacije pomembne za delovanje in poslovanje naročnika. Prav tako se na strežnikih lahko nahajajo važni poslovni in osebni podatki. Zaradi tega so strežniški sistemi kritični z vidika varnosti in je potrebno podrobno spremljati vsak dostop in obnašanje na sistemu. Strežniki se nahajajo v podatkovnem centru in tudi na centralnih lokacijah naročnika. Na vseh Windows strežnikih se dogodki zapisujejo v Event Log in sicer v Application, Security in System log. Na Linux sistemih se dogodki zapisujejo v mapo /var/log/. Beležijo se vsi dostopi do sistema in izvajanje ukazov.

4.4.2 Delovne postaje in prenosniki

Preko delovnih postaj zaposleni dostopajo do poslovnih aplikacij in tudi storitev ter vsebin na svetovnem spletu. Zaposleni nimajo administratorskih privilegijev na delovni postaji, kar pomeni, da ne morejo nameščati programske opreme in izklapljati ali spreminjati varnostnih nastavitev na sistemu. Na vseh sistemih je nameščen Microsoftov Endpoint Protection klient, ki skrbi za zaznavo virusov in druge škodljive kode, ter zaznavo napadov na končni sistem. Klient se upravlja preko centralne nadzorne naprave in uporabnik nima dostopa do njega. Prav tako se iz centralnega mesta skrbi za nastavitve delovnih postaj in njihove posodobitve. Večina delovnih postaj ima še nameščen operacijski sistem Windows 8, novejše delovne postaje pa imajo nameščeno zadnjo verzijo Windows 10. Na delovnih postajah ne tečejo poslovne aplikacije, prav tako se na njih praviloma ne nahajajo pomembni podatki. Zaradi tega delovne postaje niso kritične iz vidika varnosti, želimo pa spremljati vse prijave in odjave iz sistema ter uporabo priviligiranih ukazov. Te aktivnosti opredeljuje politika “Audit logon events”, kjer dogodki z oznakami 4624,4625,4648,4634,4647,4672 in 4778 označujejo zapise povezane s temi aktivnostmi [26]. Delovne postaje se nahajajo na centralnih in oddaljenih lokacijah, prenosnike pa lahko zaposleni odnesejo tudi izven naročnikovega okolja.

4.4.3 Podatkovne zbirke

Podatkovne zbirke nudijo platformo za različne podatkovne baze do katerih dostopajo poslovne aplikacije za potrebe obdelave poslovnih podatkov. Podatkovni strežnik je centraliziran v podatkovnem centru in vsi dostopi do njega so možni samo preko požarne pregrade. V podatkovnih bazah, ki se nahajajo na njem, so shranjeni poslovni in osebni podatki. V primeru izrabe ranljivosti sistema ali nepooblaščenega dostopa bi bili lahko podatki ogroženi, zato je sistem kritičen iz vidika varnosti in je potrebno podrobno spremljati dostope in obnašanje na sistemu. V okolju naročnika se uporablja Microsoft SQL Server 2012, na katerem se nahaja več kot pet podatkovnih baz.

4.4.4 Infrastrukturne aplikacije

Infrastrukturne aplikacije omogočajo platformo in podporne funkcije za delovanje celotnega informacijskega sistema. Aplikacije so pomembne za delovanje informacijskega sistema, same pa ne vsebujejo poslovnih ali osebnih podatkov. Ker pa ponujajo vmesnik med uporabniki in poslovnimi storitvami, bi lahko izraba nepravilne nastavitve ali ranljivosti omogočila nepooblaščen dostop in odtekanje podatkov. Prav tako bi lahko napad na te vrste aplikacij onemogočil delovanje informacijskega sistema. Zaradi tega so infrastrukturne aplikacije kritične iz vidika varnosti. Potrebno je spremljanje izrabe teh aplikacij in njihovo delovanje.

Microsoft Share Point

Microsoft Share Point je spletna platforma na kateri se nahajajo strani namenjene izmenjavi podatkov in datotek pri posameznih projektih. Do sistema imajo dostop tako zaposleni pri naročniku, kot tudi zunanji uporabniki, ki sodelujejo na projektu. Z nastavitvijo dovoljenj na aplikaciji se omogoči dostop in nivo dovoljenj za posameznega uporabnika. Uporablja se verzija Microsoft Sharepoint 2010.

Microsoft PKI

Microsoftova infrastruktura javnih ključev je namenjena izdajanju potrdil napravam in uporabnikom, ki jih potrebujejo za dostop do omrežja ali za oddaljeni dostop. V uporabi je varnostna politka, ki opredeljuje izdajanje, obnovo in preklic javnih ključev za dostop naprav in končnih uporabnikov v brezžično omrežje naročnika in oddaljeni dostop.

Spletni strežnik

Spletni strežnik nudi infrastrukturo za spletne aplikacije, ki jih ponuja naročnik. Naročnik ponuja spletno stran, ki je namenjena splošni predstavitvi naročnika, objavi reklamnih akcij in prijavi na elektronske novice ter teče na spletnem strežniku Microsoft Internet Information Server (IIS) verzije 8. Poleg tega ima naročnik tudi spletno trgovino, ki teče na strežniku Apache Web Server verzije 2.4.

VMware infrastruktura

VMware EXS je dinamična virtualizacijska infrastruktura, ki omogoča optimizirano uporabo in delitev sistemskih resoursov kot so delovni spomin, procesor, omrežja in disk med različne virtualne sisteme. VMware ESX omogoča, da na istem fizičnem strežniku paralelno teče več različnih in neodvisnih aplikacij. Z uporabo naprednih funkcionalnosti, ki jih ponuja VMware VirtualCenter, je možno centralizirano upravljanje in spremljanje delovanja ESX sistemov, vzpostavitev visoke razpoložljivosti in avtomatizacija delovanja sistema. Uporabljene so verzije VMware ESXi 6.0 Update 3 in vCenter Server 6.0 update 3b. Centralni virtualizacijski sistem je nameščen v podatkovnem centru, medtem ko se na vsaki lokaciji nahaja lokalni virtualizacijski sistem, ki služi za postavitev sistemov potrebnih na vsaki centralni lokaciji.

Datotečni strežnik

Za potrebe izmenjave datoteke med uporabniki informacijskega okolja se v posamezni državi in v podatkovnem centru nahaja strežnik z Windows operacijskim sistemom, ki opravlja vlogo datotečnega strežnika. Strežnik teče na operacijskem sistemu Windows server 2012 R2. Dostopna dovoljenja so definirana glede na vlogo posameznika znotraj Windows domene.

Aktivni imenik

Aktivni imenik močno olajša upravljanje in administracijo sistemov v informacijskem okolju. Omogoča namreč uporabo domene (angl. *domain*), ki združuje računalnike in naprave v omrežju, ki imajo skupna pravila in postopke. Aktivni imenik omogoča, da centralizirano upravljamo s pravili in postopki. Glavne funkcionalnosti, ki se uporabljajo v aktivnem imeniku, so sledeče:

- upravljanje z uporabniškimi profili,

- uveljavljanje varnostnih politik,
- dodeljevanje uporabniških pravic,
- kreiranje in spreminjanje uporabniških imen in gesel,
- dodeljevanje dostopa do omrežnih sredstev in naprav (npr. tiskalnikov),
- nastavitev skupinskih pravilnikov in organizacijskih enot.

Vsi sistemi z nameščenim Windows operacijskim sistemom so člani domene. Na samem sistemu se ne nahajajo poslovne informacije, vendar pa nekdo, ki pridobi administratorski dostop do aktivnega imenika, dostopa neomejeno skoraj do vseh informacijskih sistemov znotraj informacijskega okolja. Zaradi tega dejstva je aktivni imenik še posebej kritičen vir iz vidika varnosti.

4.4.5 Poslovne aplikacije

V informacijskem okolju se uporabljajo različne poslovne aplikacije od sistema za upravljanje odnosov s strankami (angl. *Customer Relationship Management*), sistema za vodenje zalog in skladišča, kadrovskega sistema itd. Poslovne aplikacije imajo direkten dostop do poslovnih in osebnih podatkov, zato imajo še posebej kritično mesto v informacijski varnosti. Poslovne aplikacije, ki jih uporablja naročnik, so kupljene na trgu in posebej prilagojene potrebam naročnika. Dostop do aplikacij se izvaja preko dostopnih kontrol na požarnih pregradah in z avtorizacijo dostopa do aplikacije. Avtorizacija dostopa je vgrajena tako na infrastrukturnih aplikacijah, kot tudi samih poslovnih aplikacijah. Tako na primer spletni strežnik avtorizira dostop uporabnika do poslovne aplikacije, ki teče na njem. Avtorizacija vgrajena v poslovno aplikacijo določi, do katerih podatkov in na kakšen način lahko uporabnik dostopa.

4.4.6 Mrežna in varnostna oprema

Mrežna oprema v vzorčnem okolju skrbi izključno za povezljivost med uporabniki in storitvami in ne vsebuje nobenih poslovnih informacij. Zaradi tega ni kritičen vir, vendar pa je potrebno spremljati vsak nepooblaščen dostop do in preko mrežne opreme. Varnostna oprema prav tako ne hrani poslovnih informacij, omogoča pa spremljanje in beleženje vseh aktivnosti v vzorčnem okolju in je zato kritična iz vidika varnosti.

Stikala Cisco

Cisco stikala Catalyst C3750 z operacijskim sistemom IOS 15.0 se nahajajo v podatkovnem centru. Stikala nudijo povezljivost preko povezovalne plasti do končnih sistemov in preko omrežne plasti do sistemov v drugih omrežjih. Ker gre izključno za priklop strežniških sistemov, na stikalih niso aktivirani varnostni mehanizmi. Mrežni priključki, ki niso v uporabi, so administrativno onemogočeni.

Stikala Aruba

Stikala Aruba serije 2530 se nahajajo v vseh centralnih in oddaljenih lokacijah ter nudijo povezljivost preko povezovalne plasti končnih sistemov do omrežja. Število uporabljenih stikal je odvisno od števila potrebnih mrežnih priključkov. Na centralnih lokacijah sta nameščeni med dve in šest stikal, na oddaljenih pa praviloma samo eno. Neuporabljeni mrežni priključki na stikalih so administrativno onemogočeni, na stikalih ni implementiranih drugih varnostnih mehanizmov. Omogočeni mrežni priključki so administrativno postavljeni v pravilno virtualno omrežje, tako da je komunikacija med napravami istega tipa omogočena preko stikala, komunikacija med različnimi tipi naprav pa preko usmerjevalnika na oddaljenih lokacijah ali požarne pregrade na centralnih lokacijah.

Dostopne točke Aruba

Dostopne točke Aruba 103 se uporabljajo za nudenje brezžičnega dostopa na centralnih in oddaljenih lokacijah. Posamezna dostopna točka nudi tri SSIDje (angl. *service set identifier*) za različne tipe in namene dostopa. Za uporabnike in naprave, ki so člani domene, je možna prijava s certifikati. Za znane naprave je v sistem vnešen MAC (angl. *Media Access Control*) naslov, za dostop je potrebna prijava z geslom. Za zunanje uporabnike pa je možna prijava preko registracije na spletnem portalu. Vsak SSID uporablja svoj VLAN, ki je preko dostopnega stikala speljan do naprave, ki skrbi za usmerjanje in pravila dostopa.

Požarna pregrada Check Point

Za ščitenje dostopov in možnost vzpostavljanja kriptirane povezave s poslovnimi partnerji se v podatkovnem centru uporablja požarna pregrada Check Point verzije R77.30. Vsa komunikacija do podatkovnega centra se izvaja preko te požarne pregrade, prav tako pa preko nje prehaja tudi komunikacija med centralnimi lokacijami ter med oddaljenimi

lokacijami iz različnih držav. Požarna pregrada je podvojena, pri čemer se posamezna požarna pregrada nahaja na drugi lokaciji. Poleg vloge požarne pregrade opravlja tudi vlogo posredovalnika prometa. Funkcionalnosti, ki jih nudi požarna pregrada, so naslednje:

- definiranje pravil dostopa,
- ščitenje prometa pred vdori,
- ščitenje prometa pred preobremenitvenimi napadi (angl. *denial of service attack*),
- usmerjanje prometa,
- vzpostavljanje tunelov s poslovnimi partnerji in centralnimi lokacijami,
- omogočanje oddaljenega dostopa.

Požarna pregrada se upravlja preko nadzornega sistema, ki se prav tako nahaja v podatkovnem centru. Požarna pregrada posreduje vse zaznane dostope in varnostne dogodke v nadzorni sistem, prav tako pa se spremljajo in beležijo tudi aktivnosti upravljalcev sistema.

Požarna pregrada Cisco Meraki

Na centralnih lokacijah v posamezni državi se uporablja požarna pregrada Cisco Meraki MX80 verzije MX 14.7, ki opravlja vlogo požarne pregrade in tudi vlogo posredovalnika prometa. Požarna pregrada je podvojena s tem, da se obe napravi nahajata na isti lokaciji. Uporabniki iz centralne in oddaljenih lokacij v isti državi prehajajo preko MX80 naprave direktno v internet. Iz MX80 naprave je vzpostavljen tunel do podatkovnega centra, preko katerega se izvajajo vsi dostopi do storitev v podatkovnem centru in do lokacij v drugih državah. Funkcionalnosti, ki jih nudi požarna pregrada, so naslednje:

- definiranje pravil dostopa,
- ščitenje prometa pred vdori,
- ščitenje spletnega prometa pred škodljivimi aplikacijami in virusi,
- omejevanje spletnega dostopa do prepovedanih strani,
- usmerjanje prometa,

- vzpostavljanje tunelov z oddaljenimi lokacijami in podatkovnim centrom.

Na oddaljenih lokacijah se uporablja požarna pregrada Cisco Meraki MX64 verzije MX14.7. Ta naprava nudi le funkcionalnost vzpostavljanja tunela s centralno lokacijo in omejevanje lokalnega prometa na lokaciji. Meraki rešitve se upravljajo preko nadzorne komponente, ki je nameščena v Cisco oblaku in do katere imajo dostop upravljalci sistema, ki poznajo dostopna gesla. Naprave lahko v omejenem obsegu posredujejo zapise v nadzorno komponento.

Usmerjevalnik Cisco

V podatkovnem centru se za zagotavljanje povezljivosti v internet uporabljata usmerjevalnika Cisco 4451 verzije 15.3. Usmerjevalnika se uporabljata izključno za zagotavljanje povezljivosti do svetovnega spleta preko dveh različnih ponudnikov. V ta namen je bil naročniku dodeljen neodvisni naslovni prostor (angl. *Provider Independent Address Space*), ki ga usmerjevalnika preko BGP protokola oglašujeta naprej v svetovni splet. Dostop do usmerjevalnikov je omogočen samo administratorjem sistema iz omejenih naslovov in se na napravi skupaj z izvajanimi ukazi beleži.

Poštni sistem

V podatkovnem centru se nahajata dva poštna strežnika, ki skrbita za sprejem, pregledovanje in usmerjanje elektronske pošte. Uporablja se rešitev proizvajalca ClearSwift Secure Email Gateway (SEG) verzije 4.6, ki nudi sledeče funkcije:

- sprejem in usmerjanje elektronske pošte,
- zaščito pred neželeno elektronsko pošto,
- zaščito pred virusi in škodljivo kodo v elektronski pošti,
- vsebinsko pregledovanje elektronske pošte,
- shranjevanje elektronske pošte v karantenah,
- dostop končnih uporabnikov do sporočil, ki so jim bila namenjena in se nahajajo v karantenah.

Strežnika sta postavljena v gručo (angl. *cluster*), kar pomeni, da imata skupno varnostno politiko. Upravljanje s sistemom se izvaja na napravi sami, potreben pa je dostop preko

https protokola in poznavanje ustreznih dostopnih podatkov. Posebnost rešitve SEG je ta, da se lahko gruča upravlja iz kateregakoli člana in da so zapisi povezani s sledenjem elektronske pošte vidni na obeh napravah. SEG temelji na RedHat 6 operacijskem sistemu, kar pomeni, da se vsi zapisi nahajajo v mapi /var/log.

4.4.7 Popis virov v vzorčnem okolju

V tabeli številka 4.1 so navedeni tipi in število infromacijskih sistemov, ki posredujejo svoje zapise na SIEM sistem.

4.5 Opis uporabljene SIEM rešitve

Za prikaz delovanja smo uporabili rešitev prizvajalca McAfee (Intel Security), ki že vrsto let velja za enega od vodilnih in najbolj naprednih proizvajalcev SIEM rešitev [27]. Sistem je sestavljen iz naslednjih komponent:

- Enterprise Security Manager (ESM),
- Event Receiver (ERC),
- Advanced corelation Engine (ACE),
- Enterprise Log Manage (ELM),
- Application Data Monitor (ADM),
- Database Event Monitor (DEM),
- Global Threat Intelligence (GTI).

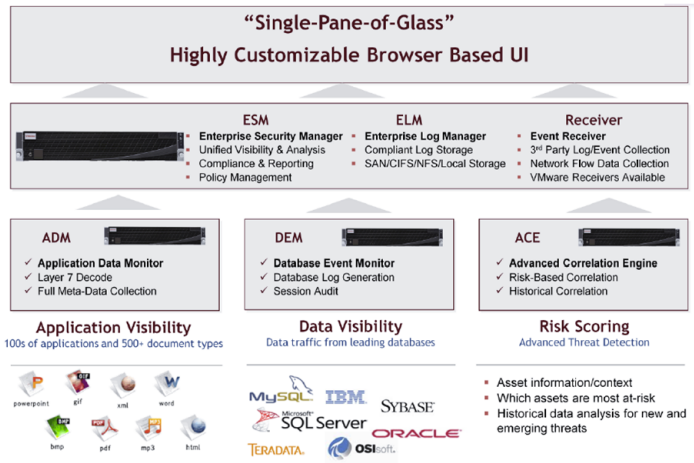
Prikaz komponent McAfee sistem sistema je prikazan na sliki 4.4.

4.5.1 Enterprise Security Manager

ESM je jedro rešitve in omogoča vpogled v delovanje SIEM sistema ter stanje varnosti nadzorovanega informacijskega sistema. Omogoča, da v realnem času identificiramo stanje sistema in reagiramo na zaznane anomalije in varnostne grožnje. Preko njega upravljamo z ostalimi komponentami sistema, izdelujemo poročila in izvajamo analize sistemov.

Sistem		Število naprav
Strežniki	Windows Server 2008	4
	Windows Server 2012	10
	Linux CentOS-7	3
Delovne postaje	Windows 8 in 8.1	188
	Windows 10	32
Podatkovne zbirke	Microsoft SQL	2
Infrastrukturne aplikacije	Microsoft SharePoint	1
	Microsoft PKI	1
	Spletni strežniki IIS	1
	Spletni strežniki Apache	1
	VMware ESX	7
	VMware Virtual Center	1
	Datotečni strežnik	5
	Aktivni imenik	2
Mrežna in varnostna oprema	Stikala Cisco	6
	Stikala Aruba	142
	Dostopne točke Aruba	280
	Požarna pregrada Check Point	2
	Požarna pregrada Cisco Meraki	130
	Usmerjevalnik Cisco	2
	ClearSwift SEG	2

Tabela 4.1 Tipi in število informacijskih sistemov v vzorčnem okolju.



Slika 4.4 Prikaz komponent McAfee SIEM sistema [28].

4.5.2 Event Receiver

ERC je komponenta, ki omogoča zbiranje in shranjevanje več kot 10.000 dogodkov na sekundo. Uporablja visoko indeksirano podatkovno bazo, ki omogoča hiter dostop do podatkov za potrebe analiz. V kompleksnih okoljih je možna distribuirana postavitev večih ERC komponent s tem, da je možna centralizirana korelacija zapisov iz večih ERCjev.

4.5.3 Advanced Corelation Engine

ACE je komponenta, ki omogoča izvajanje kompleksnih korelacij potrebnih za zaznavo naprednih napadov v realnem času. Zaznava je možna na osnovi pravil, ali pa na analizi tveganj, pri kateri specificiramo najbolj kritične vire v našem informacijskem sistemu. Komponenta omogoča tudi uporabo revizijskih sledi in predvajanje shranjenega prometa za potrebe dodatnih analiz ali dokazovanj.

4.5.4 Enterprise Log Manager

ELM je opcijska komponenta, ki omogoča dolgoročno shranjevanje zapisov. Njena naloga je da zbira, kompresira, podpisuje in shranjuje vse izvirne dogodke z jasno revizijsko sledjo dejavnosti, ki je ni mogoče zavrniti.

4.5.5 Application Data Monitor

ADM komponenta omogoča spremljanje uporabe aplikacij vse do sedmega OSI nivoja. Omogoča odkrivanje goljufij, odtekanja podatkov in naprednih groženj, pri uporabi sicer dovoljenih poslovnih aplikacij. Prav tako omogoča shranjevanje celotnega aplikativnega prometa za potrebe revizijskih sledi.

4.5.6 Database Event Monitor

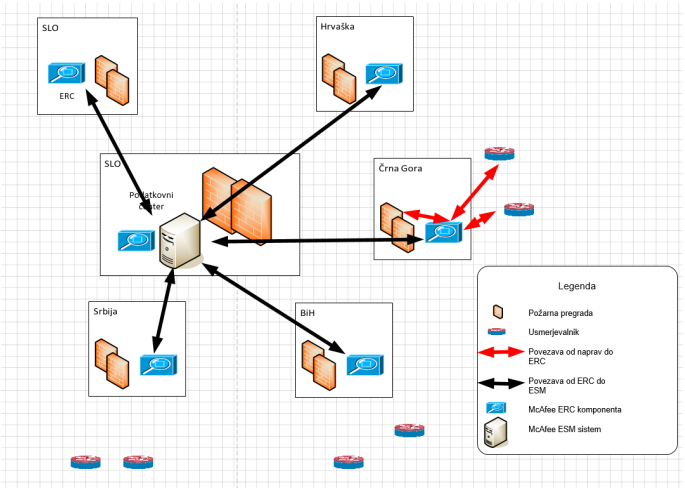
DEM je komponenta, ki omogoča popolno revizijsko sled aktivnosti podatkovnih zbirk. Spremlja lahko izvajanje poizvedb vključno z vrnjenimi rezultati, kdo se prijavlja na sistem in kam dostopa ter aktivnosti, ki jih izvaja.

4.5.7 Global Threat Intelligence

GTI je spletna storitev, ki omogoča uporabo spletnih virov (angl. *feed*) v SIEM rešitvi. Z integracjio GTI komponente v SIEM lahko ugotovimo komunikacijo s sumljivimi ali škodljivimi strežniki v realnem času. Analitiki lahko analizirajo tudi shranjene zapise in ugotavljajo pretekle interakcije s škodljivimi strežniki.

4.6 Umestitev SIEM rešitve v vzorčno okolje

Zaradi distribuiranega okolja in optimizacije podatkovnih tokov, se je na vsako lokacijo namestila komponenta za sprejemanje zapisov - ERC. V komponento so se povezale naprave iz iste države, z izjemo Slovenije, kjer se je uporabila ena ERC komponenta za centralno in oddaljene lokacije in druga ERC komponenta za podatkovni center. V podatkovnem centru so se namestile tudi preostale uporabljene komponente McAfee SIEM rešitve: ESM, ACE in ADM. Lokalni ERC sistemi so se povezali v centralni ESM sistem, preko katerega se izvaja korelacija zabeleženih zapisov in zaznavanje napadov. Prav tako se celotno upravljanje s sistemom izvaja preko centralnega ESM sistema. Vsi uporabljeni sistemi so nameščeni v VMware ESX okolja uporabljena na centralnih lokacijah in podatkovnem centru. Na sliki 4.5 je prikazana umestitev komponent SIEM sistema v vzorčno okolje.



Slika 4.5 Prikaz umestitev SIEM rešitve v vzorčno okolje.

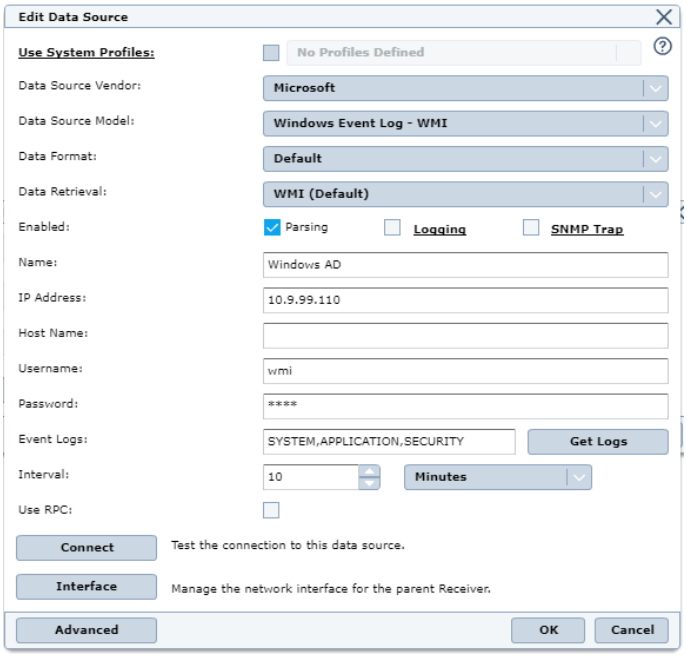
4.7 Povezava virov v SIEM rešitev

Da bi lahko dogodke, ki jih zaznajo posamezni sistemi, povezovali in znotraj njih iskali korelacije in da bi se izognili nevarnosti spreminjanja ali brisanja zapisov na samem viru zaznave, je potrebno zapise posredovati na centralni SIEM sistem. Razdelek opisuje postopke nastavitev, ki jih je potrebno narediti tako na viru, kot tudi na samem SIEM sistemu, da se zapisi posredujejo na SIEM sistem in da jih le ta pravilno obdela.

4.7.1 Windows operacijski sistemi

Postopek vključitve velja za vse strežnike in delovne postaje z operacijskim sistemom Microsoft Windows od Windows XP in Server 2003 naprej in omogoča posredovanje Windows Event Loga preko WMI. Za potrebe vključitve posameznega sistema Windows v sistem zbiranja zapisov preko McAfee SIEM sistema kreiramo poseben uporabniški račun, ki ga dodamo v administratorsko skupino znotraj domene. Nastavitve potem distribuiramo preko skupinskih politik (angl. *group policy*). S tem omogočimo, da nastavitve veljajo tudi za računalnike, ki jih naknadno vključimo v domeno.

Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver- ELM ter izberemo lastnosti in Data Sources. V oknu, ki se nam odpre, dodamo nov vir, kot je prikazano na sliki 4.6.



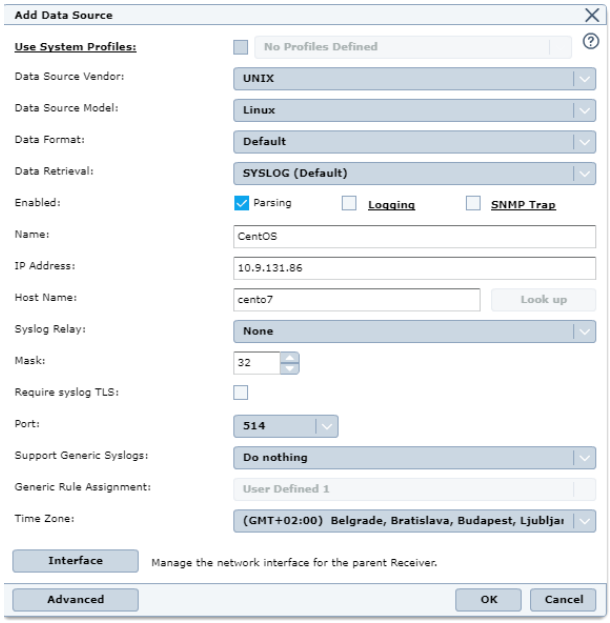
Slika 4.6 Prikaz nastavitev vira Microsoft v McAfee ESM.

4.7.2 Linux operacijski sistem

Za potrebe vključitve strežnikov s CentOS operacijskim sistemom moramo preusmeriti syslog promet na ERC strežnik, kar naredimo po naslednjem postopku:

- prijavimo se na strežnik in gremo v root način,
- spremenimo */etc/rsyslog.conf* datoteko tako, da dodamo vrstico **.* @@IP NASLOV ERC:514*,
- ponovno zaženemo syslog servis z izvedbo ukaza */bin/systemctl restart rsyslog.service*.

Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver-ELM ter izberemo Add Data Source. V okno, ki se nam odpre, vnesemo vrednosti, kot je prikazano na sliki 4.7. Za posredovanje zapisov iz strežnikov s CentOS operacijskim sistemom je potrebno odpreti tudi komunikacijsko pot med sistemoma in sicer moramo omogočiti promet UDP 514 iz strežnikov do ERC.



Slika 4.7 Prikaz nastavitev vira s CentOS operacijskim sistemom v McAfee ESM.

4.7.3 Požarna pregrada Check Point

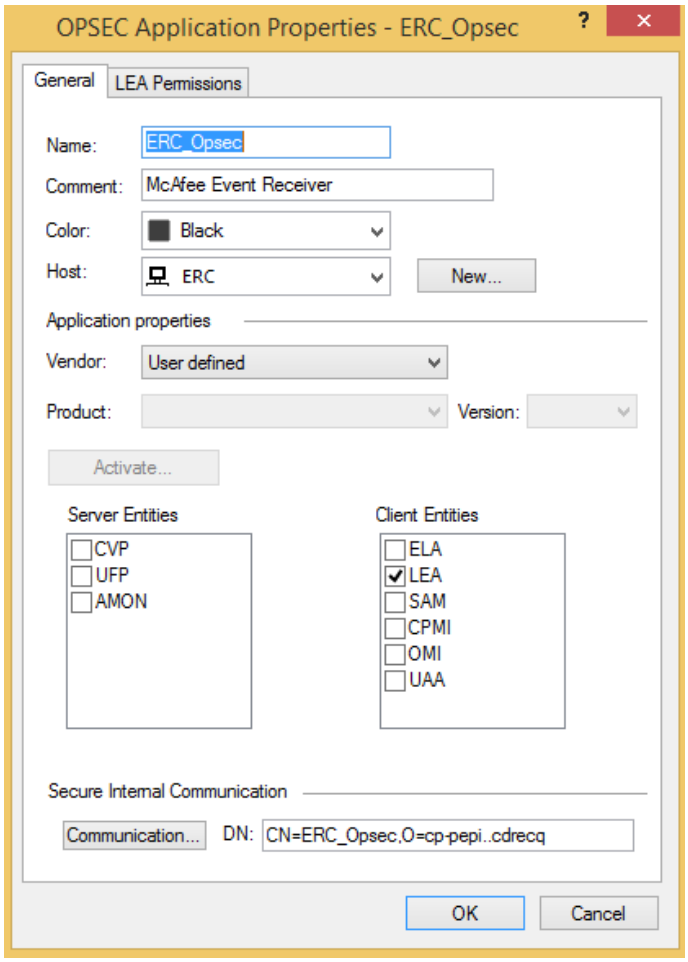
Za potrebe vključitve požarne pregrade Check Point moramo slediti naslednjemu postopku. Na upravljalnem strežniku požarne pregrade omogočimo LEA servis. Na upravljalni strežnik se prijavimo preko SSH protokola in gremo v EXPERT način. Spremenimo datoteko $FWDIR/conf/fwopsec.conf tako, da dodamo vrstici prikazani v zapisu 4.1.

Zapis 4.1 Omogočanje fwopsec komunikacije na požarni pregradi Check Point.

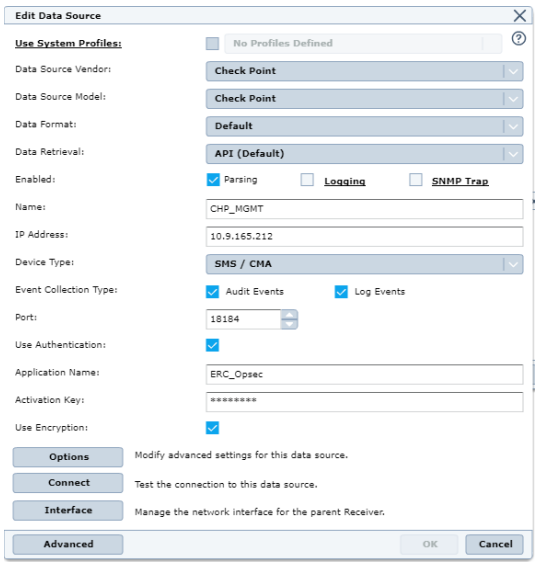
```
lea\_server auth\_port 18184
lea\_server auth\_type ssl\_ca
```

in ponovno zaženemo servis. S tem omogočimo kriptirano in avtenticirano povezavo med upravljalnim strežnikom požarne pregrade in oddaljenimi sistemi. Na upravljalni strežnik se sedaj prijavimo preko konzole imenovane SmartDashboard. Kreiramo novo OPSEC aplikacijo z nastavitvami, kot so prikazane na sliki 4.8, ter shranimo bazo na upravljanem strežniku. Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver - ELM ter izberemo lastnosti in Data Sources. V oknu, ki se nam odpre, dodamo nov vir, kot je prikazano na sliki 4.9.

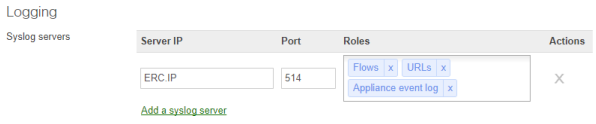
Ko dodamo vir, izvedemo akcijo Connect in počakamo, da se vzpostavi povezava med virom in ERC. Za posredovanje zapisov iz Check Point požarne pregrade je po-



Slika 4.8 Prikaz nastavitve OPSEC aplikacije na požarni pregradi Check Point.



Slika 4.9 Prikaz nastavitev vira Checkp Point v McAfee ESM.



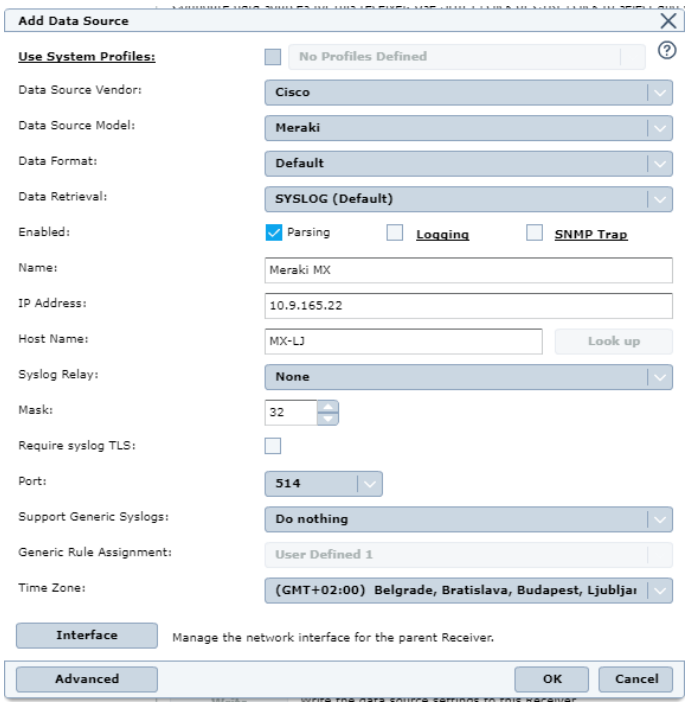
Slika 4.10 Prikaz nastavitve "syslog" strežnika na požarni pregradi Meraki.

trebno odpreti tudi komunikacijsko pot med sistemoma in sicer je potrebno omogočiti dostop po portih FW_ICA_Pull (TCP 18210) in FW_Lea (TCP 18184) iz ERC sistema do upravljalnega strežnika Check Point.

4.7.4 Požarna pregrada Meraki

Za potrebe vključitve požarne pregrade Meraki se je potrebno z brskalnikom prijaviti v nadzorni sistem, ki se nahaja v oblaku. Izberemo Network-wide in nato Configure ter General in dodamo "syslog" strežnik, kot je prikazano na sliki 4.10.

Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver- ELM ter izberemo lastnosti in Data Sources. V oknu, ki se nam odpre, dodamo nov vir, kot je prikazano na sliki 4.11. Za posredovanje zapisov iz Meraki požarne pregrade je potrebno odpreti tudi komunikacijsko pot med sistemoma in sicer moramo omogočiti promet UDP 514 iz Meraki naprav do ERC.



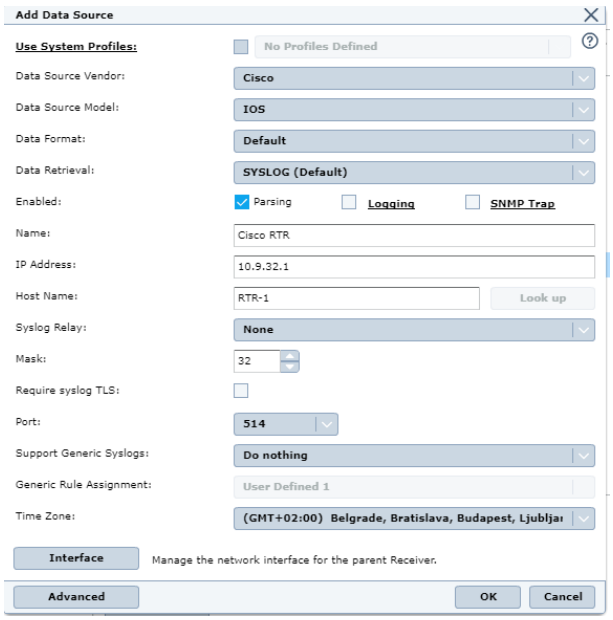
Slika 4.11 Prikaz nastavitev vira Meraku v McAfee ESM.

4.7.5 Mrežna oprema Cisco IOS

Postopek vključitve za mrežno opremo Cisco IOS velja tako za stikala, kot tudi usmerjevalnike Cisco. Koraki, ki jih moramo izvesti, so naslednji:

- prijava na napravo in prehod v "enable" način,
- prehod v konfiguracijski način z izvedbo ukaza *configure terminal*,
- vklop zapisovanja z izvedbo ukaza *logging on*,
- posredovanje zapisov na ERC sistem z izvedbo ukaza *logging IP NASLOV ERC*,
- vklop časovnega žigosanja zapisov z izvedbo ukaza *service timestamps log datetime localtime*,
- prilagoditev nivoja zapisovanja z izvedbo ukaza *logging trap warning*.

Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver-ELM ter izberemo lastnosti in Data Sources. V oknu, ki se nam odpre, dodamo nov vir, kot je prikazano na sliki 4.12.

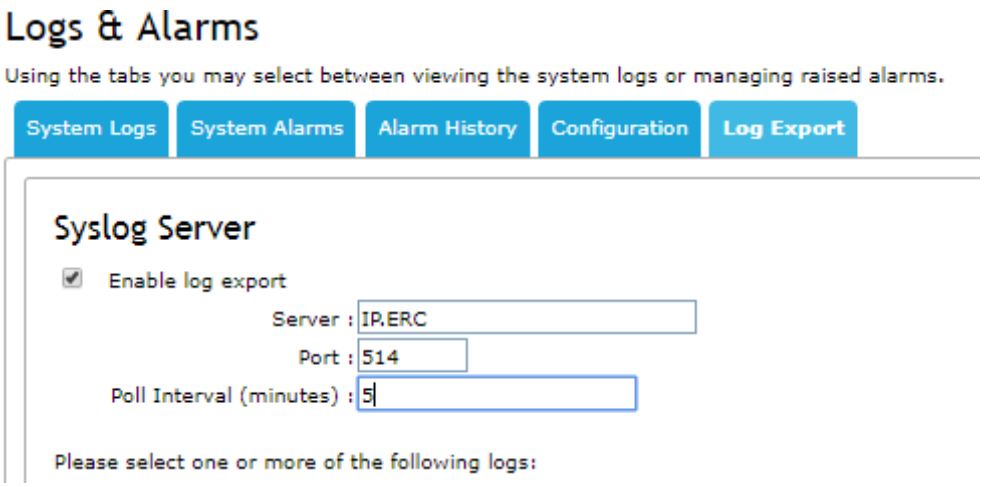


Slika 4.12 Prikaz nastavitev vira Cisco IOS naprav v McAfee ESM.

4.7.6 Poštni sistem

Za potrebe vključitve pogramske opreme CleasrSwift Secure Email Gateway (SEG) je potrebno omogočiti posredovanje zapisov na zunanji syslog strežnik preko syslog protokola. Omenjeno spremembo izvedemo tako, da se z brskalnikom prijavimo na upravljalski vmesnik SEG z vpisom naslova: https://IP NASLOV SEG/ v naslovno vrstico, izberemo System in nato Logs and Alarms ter izberemo zavihek Log Export. V oknu, ki se nam odpre, omogočimo polje Enable Log Export in vnesemo podatke ERC komponente, kot je prikazano na sliki 4.13. Izberemo tudi zapise, ki naj se posredujejo na ERC strežnik. Izberemo naslednje zapise:

- Infrastructure,
- Kaspersky Updater,
- PMM End User Operations,
- PMM Infrastructure,
- SMTP,
- Sophos Scanner,



Slika 4.13 Prikaz nastavitev Sysloga na SEG sistemu.

- Sophos Updates.

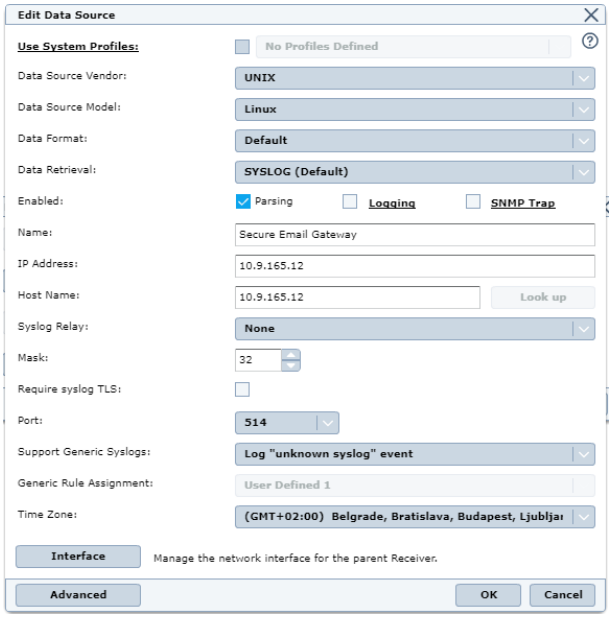
Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver-ELM ter izberemo Add Data Source. V okno, ki se nam odpre, vnesemo vrednosti, kot je prikazano na sliki 4.14.

Za posredovanje zapisov iz SEG do ERC sistema je potrebno odpreti tudi komunikacijsko pot med sistemoma in sicer mora biti omogočen promet UDP port 514 iz SEG strežnikov do ERC sistema.

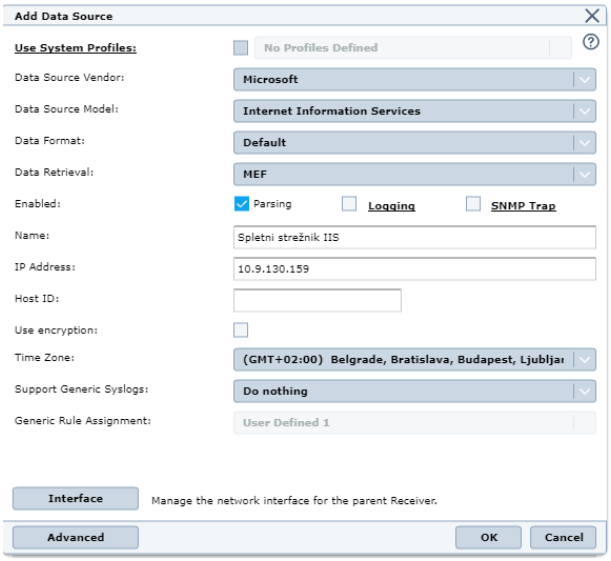
4.7.7 Spletni strežnik

Za potrebe vključitve spletnega strežnika, ki teče na Microsoft Internet Information Services (IIS) platformi, je poleg zajema Windows Event Loga opisanega v poglavju o Windows sistemih, potrebno omogočiti tudi beleženje zapisov na spletnem strežniku. To izvedemo tako, da se prijavimo v nadzorno ploščo na Windows strežniku, izberemo administrativna orodja in odpremo Internet Information Services (IIS) Manager komponento. Izberemo logiranje in W3C izpis pri katerem omogočimo vsa polja.

Po prijavi na ESM sistem izberemo zavihek Configuration in se postavimo na Local Receiver-ELM ter izberemo Add Data Source. V okno, ki se nam odpre, vnesemo vrednosti, kot je prikazano na sliki 4.15. Za potrebe vključitve spletnega strežnika, ki teče na Apache WebServer platformi, se enako kot za Linux sisteme uporabi posredovanje zapisov preko Sysloga. Dodatno moramo omogočiti beleženje zapisov spletnega strežnika



Slika 4.14 Prikaz nastavitev vira ClearSwift SEG v McAfee ESM.



Slika 4.15 Prikaz nastavitev vira spletni strežnik IIS v McAfee ESM.

in prilagoditi strukturo zapisov, kar naredimo v naslednjih korakih:

- odpremo datoteko */usr/httpd/httpd.conf*,
- spremenimo vrstico, ki določa format zapisovanja: *LogFormat "%h %l %u %t \"%r\" %>s %b \"%{REFERER }i\"\"%{User–data source}i\""combined*
- preusmerimo zapisovanje Apache WebServer v syslog.

Na strani ESM ni potrebne dodatne konfiguracije za sprejem zapisov.

4.7.8 Obogatitev podatkov

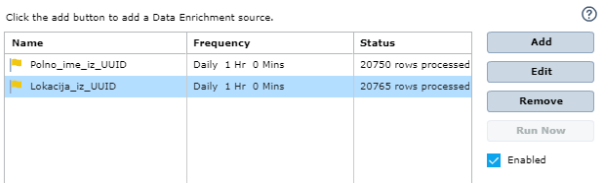
Obogatitev podatkov omogoča, da prejetim zapisom dodamo kontekst, ki ni zajet v samem zapisu. Tako lahko dodamo podatke o lokaciji in kritičnosti naprave, telefonski številki in poštnem naslovu uporabnika itd. V vzorčnem okolju smo obogatili zapise iz Windows sistemov s polnim imenom uporabnika in lokaciji delovnega mesta. Prijavili smo se v ESM konzolo in izbrali "System Properties" ter izbrali "Data Enrichment". Odprl se nam je čarovnik (angl. *wizard*) za obogatitev podatkov, v katerem smo izbrali naslednje nastavitve:

- vpisali smo ime obogatitve,
- za tip poizvedbe in tip obogatitve smo izbrali "String",
- izbrali dnevno frekvenco izvajanja,
- za tip poizvedbe smo izbrali LDAP in vpisali potrebne pristopne podatke (IP naslov, vrata, uporabnik, geslo),
- vpisali podatke za LDAP poizvedbo,
- izbrali Windows sisteme vključene v ESM kot cilje obogatitve.

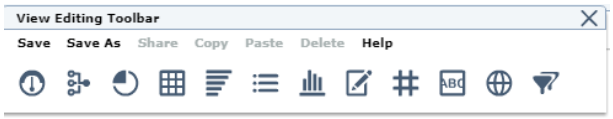
Slika 4.16 prikazuje nastavitve obogatitve podatkov v vzorčnem okolju.

4.8 Uporaba rešitve

Z vključitvijo virov v SIEM sistem postane slednji centralno mesto, na katerem lahko spremljamo celovito dogajanje v informacijskem sistemu. Zaradi množice podatkov, ki se zbirajo, je pomembno, da sistem prilagodimo tako, da so pomembne informacije takoj



Slika 4.16 Obogatitev podatkov v McAfee ESM.



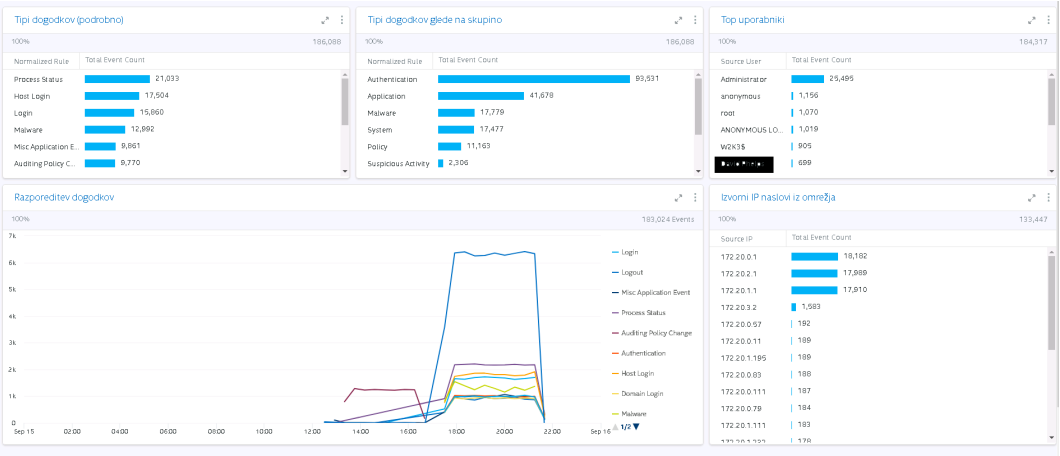
Slika 4.17 Orodna vrstica s katero gradimo nov pogled v ESM sistemu.

vidne. S tem omogočimo uporabnikom sistema hitro in efektivno delo. V poglavju so opisani postopki izgradnje prilagojenega pogleda in trije postopki uporabe sistema za zaznavanje sumljivih aktivnosti v vzorčnem informacijskem okolju.

4.8.1 Priprava prilagojenih pogledov

Prilagodljivost pogledov je pomembna lastnost SIEM sistema. Zaradi različnih vlog uporabnikov in različnih potreb po pregledu stanja je pomembno, da lahko vnaprej pripravimo poglede prilagojene zahtevam uporabnikov. V nadaljevanju je opisan postopek priprave pogleda, ki nam omogoča hitri pregled nad stanjem varnosti v sistemu. Prijavimo se v ESM nadzorno ploščo in izberemo "Configuration" ter kreiramo nov pogled z izbiro "Create New View". Odpre se nam prazno okno v katerega umestimo želene gradnike. To naredimo preko orodne vrstice za urejanje pogledov, ki je prikazana na sliki 4.17. Pogled poimenujemo Krovni pogled in vanj dodamo naslednje gradnike:

- tipe dogodkov glede na skupino (npr. sistemski dogoki, avtentikacija ipd.),
- podroben tip dogodka (npr. prijave in odjave iz sistema, prijava preko omrežja, politika sledenja na operacijskem sistemu itd.),
- časovna razporeditev dogodkov v okolju,
- uporabnike, ki generirajo največ dogodkov,
- izvorne IP naslove iz omrežja, ki generirajo največ dogodkov.

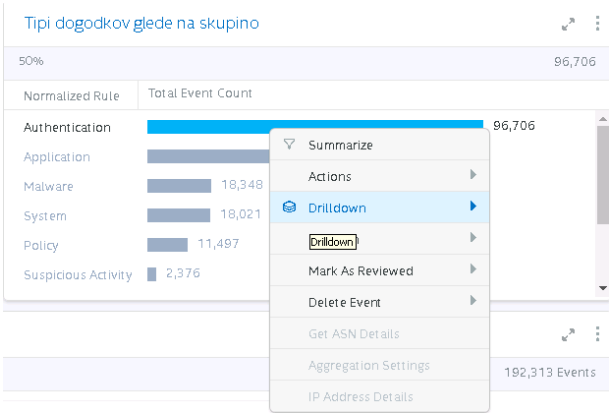


Slika 4.18 Prikaz kreiranega Krovnega pogledad.

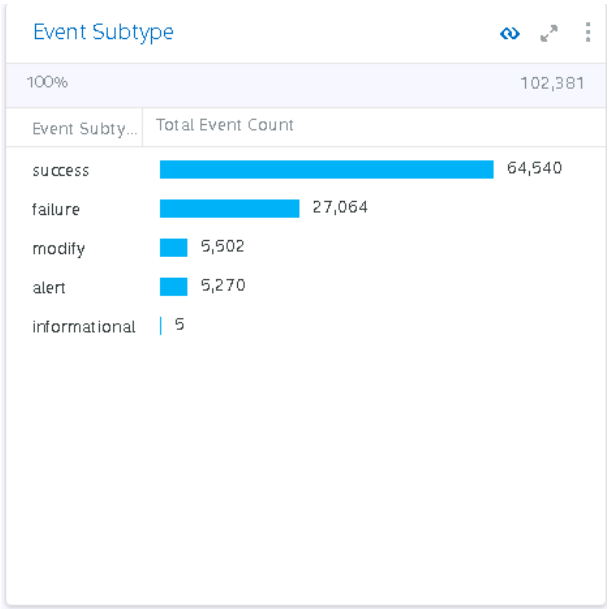
Krovni pogled nam prikaže pregled zaznanih varnostnih dogodkov v informacijskem sistemu in je osnova za nadaljno analizo in raziskovanje. Pogled je prikazan na sliki 4.18.

4.8.2 Vrtanje v globino

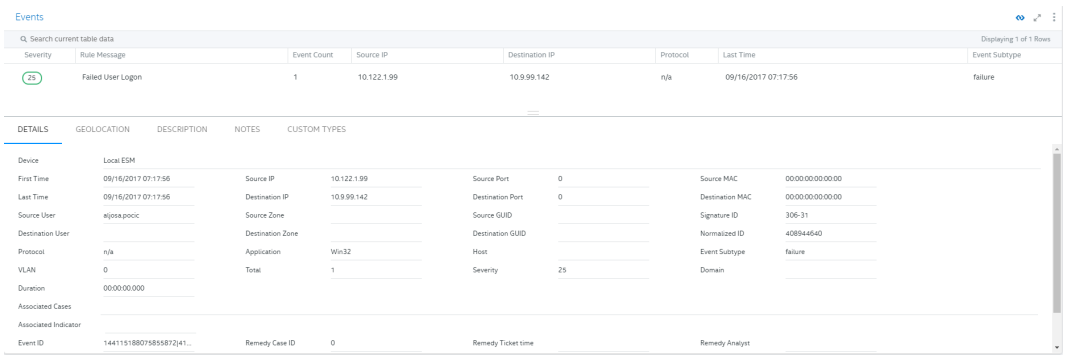
Iz krovnega pogleda dobimo globalni vpogled v okolje. Vidimo kako se giblje število dogodkov skozi čas, kateri dogodki se prožijo in kdo jih generira. Če želimo določen dogodek raziskati, pa lahko uporabimo vrtanje v globino, ki ga omogoča ESM. Tako nas zanima zakaj se proži toliko dogodkov tipa “Authentication”. V pogledu izberemo “Authentication” in nato desni klik. V oknu, ki se nam odpre, izberemo “Drildown” do podtipa dogodka, kot je prikazano na sliki 4.19. Po izvedenem koraku se nam odpre nov gradnik, ki prikazuje v fazi vrtanja izbrane podatke. Tako lahko sedaj podrobneje vidimo iz katerih podtipov dogodkov, je sestavljen tip “Authentication”. V našem primeru so to dogodki podtipov uspeh, napaka, sprememba, opozorilo in informativno, kot je razvidno iz slike 4.20. Raziskovanje dogodkov lahko še nadaljujemo, tako da izberemo na primer “failure”, desno kliknemo, izberemo “Drildown” do ciljnega IP naslova itd., dokler ne želimo videti dogodke, ki ustrezajo našim izbiram. Takrat v postopku vrtanja izberemo dogodke (angl. *Events*). Slika 4.21 prikazuje podrobnosti dogodka, do katerih lahko pridemo z vrtanjem v globino.



Slika 4.19 Postopek vrtanja v globino iz krovnega pogleda.



Slika 4.20 Prikaz novega gradnika po vrtanju v globino.



Slika 4.21 Podrobnosti dogodka neuspešne prijave na sistem.

4.8.3 Zaznavanje sumljivih akvitnosti v vzorčnem sistemu

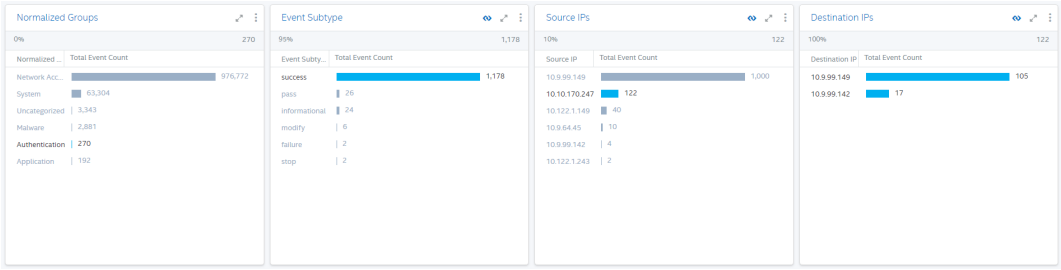
SIEM omogoča ogromno možnosti pri spremljanju in analizi zaznanih dogodkov. Katere uporabi skrbnik sistema, je odvisno od njegovih nalog in tudi od lastnosti informacijskega okolja ter njegove pomembnosti v poslovnem procesu. V razdelku bom prikazal tri tipična področja analiz, ki jih skrbniki izvajajo v SIEM sistemu. Ta tri področja so:

- spremljanje aktivnosti uporabnika,
- spremljanje uporabe spletnega prometa v neposlovne namene,
- iskanje naprednih napadov.

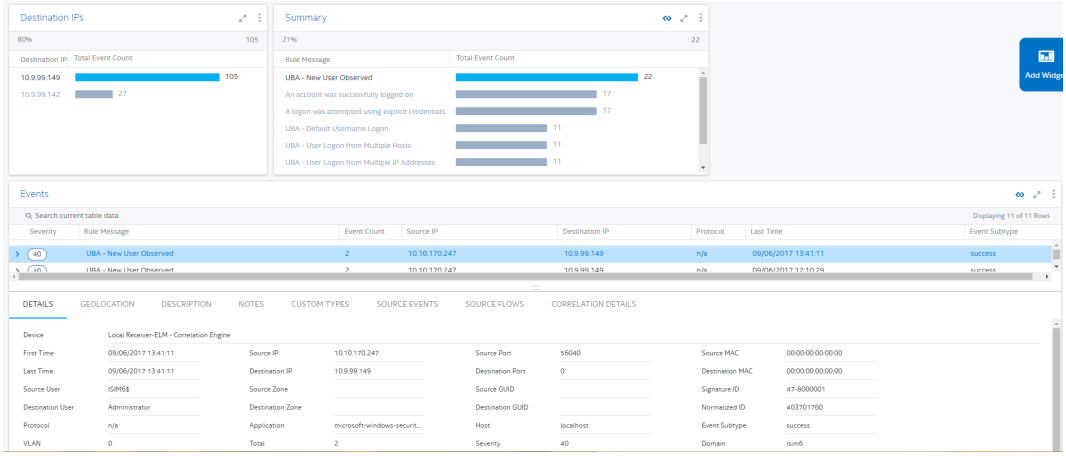
Spremljanje aktivnosti uporabnika

Eden od osnovnih primerov uporabe SIEM sistema je spremljanje aktivnosti uporabnika, z namenom zgodnjega odkrivanja dogodkov, ki bi lahko vplivali na varnost in produktivnost uporabnikov, storitev in celotnega informacijskega sistema. Dogodki, kot so zaklenjeni in onemogočeni računi, so lahko zgodnja opozorila težav. Podrobneje je opisano spremljanje uspešnih prijav na sisteme v informacijskem okolju. Praviloma so uspešne prijave aktivnost, ki jo pričakujemo v vsakem informacijskem sistemu, lahko pa pomenijo tudi neavtorizirano pridobitev dostopnih podatkov. Postopek analize je naslednji:

- prijavimo se v ESM sistem in izberemo “Authentication”,
- izberemo podtip dogodka “success”,
- izberemo izvorni IP naslov,



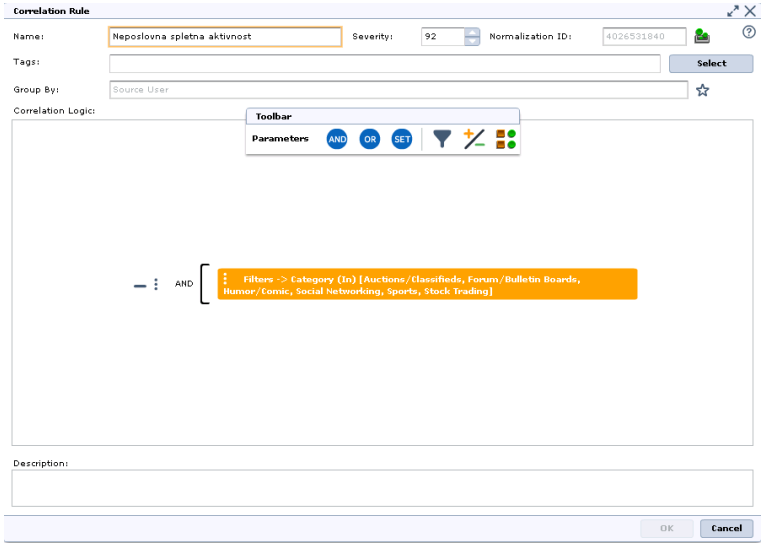
Slika 4.22 Postopek vrtanja v globino.



Slika 4.23 Postopek vrtanja v globino do končnih dogodkov.

- IP naslov 10.9.99.149 je strežnik, katerega vloga je preverjanje stanja in posodabljanje Windos operacijskih sistemov, zato je veliko število prijav iz tega naslova pričakovano,
- IP naslov 10.10.170.247 pripada brezžičnemu omrežju, zato se odločimo, da bomo podrobneje preverili te dogodke,
- izberemo ciljne IP naslove in ugotovimo, da se povezuje na dva strežnika iz mreže 10.9.99.0/24 (postopek je prikazan na sliki 4.22),
- izberemo ciljni IP naslov 10.9.99.149 in pregledamo dogodke, ki so se zgodili, kot je prikazano na sliki 4.23.

Pri analizi dogodkov je bilo ugotovljeno, da je administrator prenašal pakete na končni strežnik preko skripte in za oddaljeni dostop uporabljal uporabnika ISIM6$. V tem primeru je šlo za regularno delovanje. Preostali pogostejši primeri uporabe iz tega področja



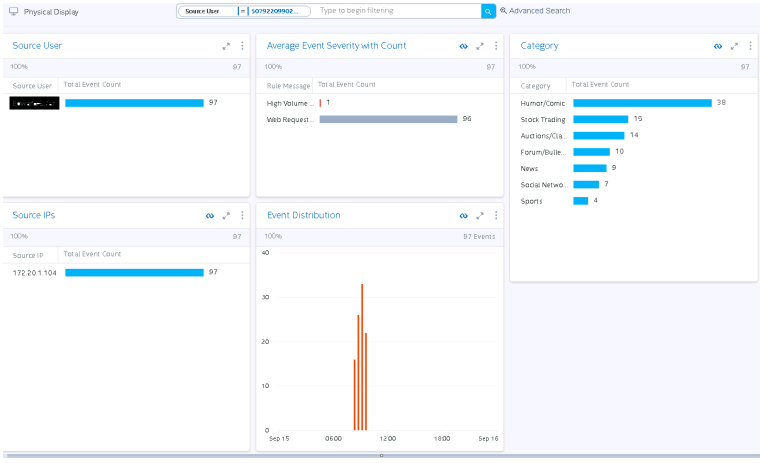
Slika 4.24 Primer korelacijskega pravila.

so:

- uporabnik pokliče na službo za pomoč uporabnikom, da se ne more prijaviti v sistem ali aplikacijo; preko SIEM sistema lahko z enostavno poizvedbo preverimo ali obstajajo dogodki kot sta pretečeno geslo ali zaklenjen račun za uporabnika;
- spremljanje uporabe pretečenih gesel v ESM konzoli za sistemske ali aplikativne račune; s spremljanjem teh dogodkov lahko enostavno ugotovimo, na katerih napravah se niso posodobila gesla za dostop do aplikacij;
- spremljanje prijav na sisteme z istim uporabniškim računom iz različnih lokacij ali naprav v kratkem časovnem obdobju;

Spremljanje uporabe spletnega prometa v neposlovne namene

V vzorčnem okolju je dostop brskanja po svetovnem spletu deloma omejen. Onemogočen je dostop do škodljivih spletnih strani in do strani z oporečno vsebino. Dostop do strani z video vsebinami, novicami ipd. ni omejen, obstaja pa pravilnik o uporabi spleta, ki omejuje uporabo v privatne namene na največ pol ure dnevno. S tem se želi preprečiti neproduktivnost zaposlenih. Najprej pripravimo korelacijsko pravilo, v katerega dodamo kategorije spletnih strani, ki niso poslovno usmerjene, kot je prikazano na sliki 4.24. Po prijavi v EMS sistem izberemo tip dogodkov “Neposlovna spletna aktivnost”. V pogledu



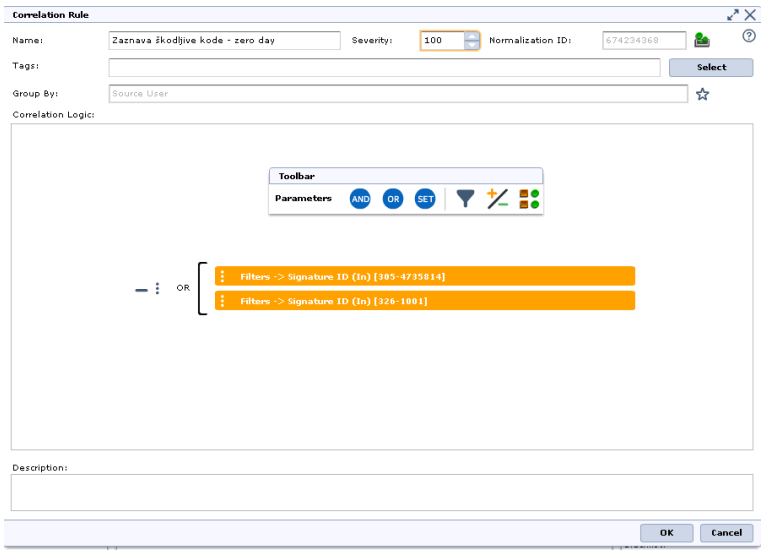
Slika 4.25 Primer pregleda spletne aktivnosti za uporabnika.

vidimo uporabnike, ki so generirali dogodek. Izberemo uporabnika in nato skupen pogled njegovih aktivnosti. Odpre se nam novo okno v katerem vidimo kdo in kdaj je uporabljal splet v neposlovne namene. Da pa bi videli tudi ciljne kategorije, izberemo vrtanje v globino nad poljem uporabnika in izberemo parameter "Category". Pogled, ki smo ga naredili, je prikazan na sliki 4.25. Pogled lahko izvozimo iz sistema v pdf obliki in ga posredujemo osebam odgovornim za uporabo spletnega prometa. Drug podoben primer iz tega področja je pregled izvornih IP naslovov iz lokalnega omrežja, ki poizkušajo doseči škodljive spletne strani. Strani so sicer blokirane in jih uporabniki ne morejo doseči, vendar pa lahko večje število poizkusov iz enega naslova pomeni, da na sistemu teče škodljiva koda, ki poizkuša priti v stik s kontrolnim centrom.

Iskanje naprednih napadov

Napredni napadalci poizkušajo na različne načine pridobiti dostop do napadenega informacijskega okolja. Pri tem poizkušajo prikriti svoje aktivnosti in biti čim dlje neopaženi. Značilna je faza priprave na napad, v kateri napadalci pridobijo kar največ javno dostopnih informacij o napadenem okolju. Primer teh informacij so:

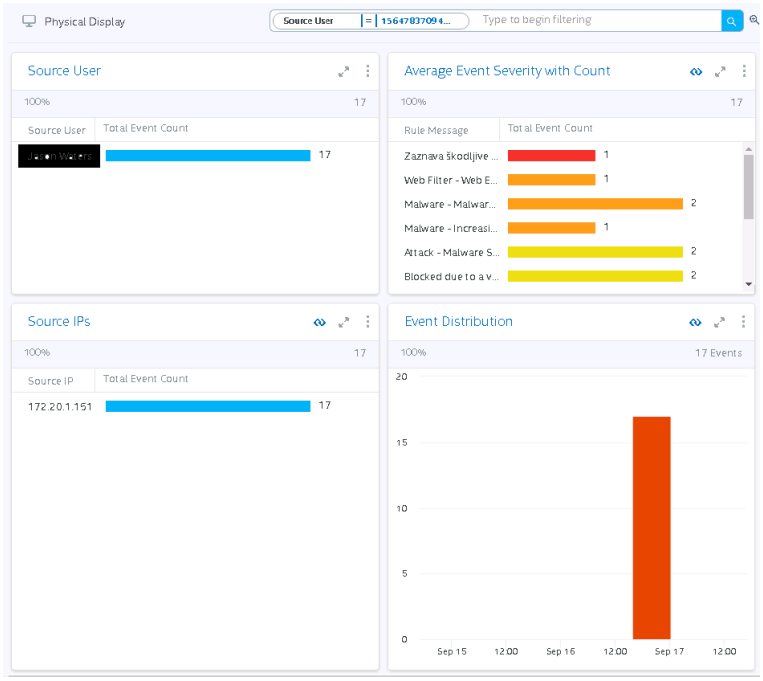
- ključne osebe v organizaciji (uprava, marketing, finance, itd.),
- poslovni partnerji,
- zunanji vzdrževalci,
- uporabljena informacijska tehnologija,



Slika 4.26 Primer korelacijskega pravila.

- uporabljena delovna sredstva,
- itd.

Po pridobljenih informacijah pripravijo usmerjen napad samo na točno določeno organizacijo ali skupino organizacij, ki imajo skupne lastnosti (npr. banke iz neke regije). V vzorčnem okolju uporabljamo požarno pregrado Check Point, katere funkcionalnost emulacije groženj (angl. *threat emulation*) omogoča detekcijo usmerjenih napadov. Vnaprej smo pripravili korelacijsko pravilo "Zaznava škodljive kode - zero day" v katerega smo dodali oznake emulacije groženj iz požarne pregrade, kot je prikazano na sliki 4.26. Po prijavi v ESM sistem izberemo tip dogodkov "Zaznava škodljive kode - zero day". V pogledu vidimo uporabnike, ki so generirali dogodek. Izberemo uporabnika in nato skupen pogled njegovih aktivnosti. Odpre se nam novo okno v katerem vidimo uporabnika, IP naslov in čas zaznave dogodkov, kot je prikazano na sliki 4.27. Razvidno je, da je bilo v kratkem časovno obdobju zaznanih 17 dogodkov. To kaže na delovanje škodljive programske opreme, ki je očitno poizkušala prenesti dodatno škodljivo kodo. Po teh ugotovitvah smo okužen sistem umaknili iz omrežja in iz njega odstranili škodljivo programsko opremo. Dodatno nas je zanimalo kako je prišlo do okužbe sistema. Preko ESM smo naredili poizvedbo za okuženega uporabnika in ugotovili, da je v času okužbe prejel štiri sporočila. Pri dodatni raziskavi smo ugotovili, da je bilo sporočilo z oznako MID



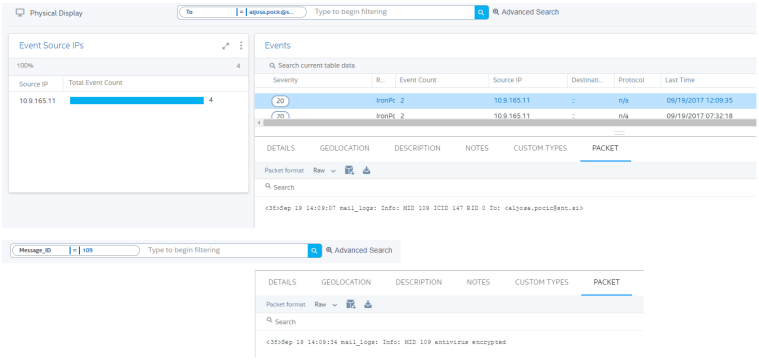
Slika 4.27 Prikaz zaznave škodljive kode.

109 kriptirano. Ker je v politiki poštnega strežnika nastavljeno, da se kopija kriptirane pošte shrani v karanteno, original pa posreduje prejemniku, smo na poštnem sistemu preverili dodatne informacije o tem sporočilu. Poizvedbe narejene na ESM sistemu so prikazane na sliki 4.28. Najprej smo preverili iz katerega naslova je prišlo sporočilo. Iz glave sporočila prikazane v zapisu 4.2 je razvidno, da je sporočilo posredoval strežnik z IP naslovom 136.243.90.167.

Zapis 4.2 Zapis glave iz prejetega sporočila.

```
Received: from dedicate.twoyellowfeet.gr (dedicate.twoyellowfeet.gr [136.243.90.167])
    by mail.vzorcno-okolje.si (8.14.7/8.14.7) with ESMTP id v8BK4mxm049825
    (version=TLSv1/SSLv3 cipher=DHE-RSA-AES256-GCM-SHA384 bits=256 verify=NO)
    for <prodaja@inotherm.si>; Mon, 11 Sep 2017 22:04:49 +0200
Message-Id: <201709112004.v8BK4mxm049825@mail.vzorcno-okolje.si>
Received: from [104.171.115.121] (port=60970)
    by dedicate.twoyellowfeet.gr with esmtpsa (TLSv1:DHE-RSA-AES256-SHA:256)
    (Exim 4.89)
    (envelope-from <info@lineastrom.gr>)
    id 1drQEd-0006TC-HM; Mon, 11 Sep 2017 18:02:52 +0300
```

IP naslov pošiljatelja smo preverili z javno dostopnimi orodji na svetovnem spletu. Spletna stran mxtoolbox.com je pokazala, da se IP naslov nahaja na eni RBL listi, kot je prikazano na sliki 4.29. Ta podatek še ni dovolj, da bi lahko z gotovostjo trdili, da gre za škodljiv poštni strežnik, saj za 89 list strežnik ni sumljiv. Zato smo dodatno preve-



Slika 4.28 Primer poizvedb na ESM.

Slika 4.29 Pregled IP naslova pošiljatelja na spletni strani mxtoolbox.

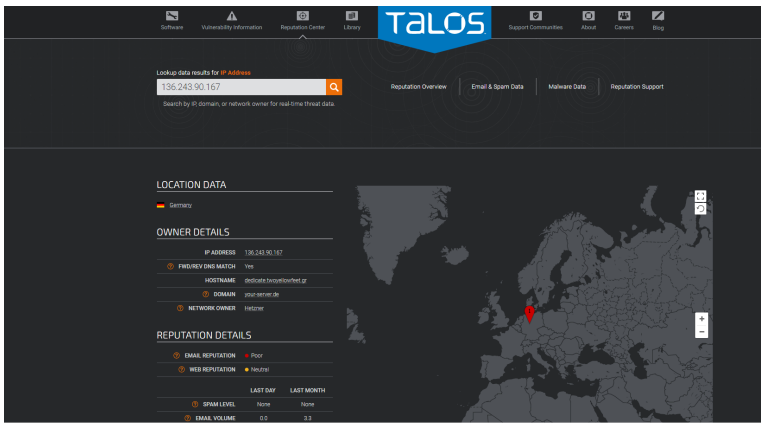
rili IP naslov na strani talosintelligence.com, kot je prikazano na sliki 4.30. Na spletni strani je viden slab ugled strežnika pri pošiljanju elektronske pošte, vendar pa strežnik ni klasificiran kot pošiljatelj spam sporočil.

Glede na vsebino sporočila, ki je prikazana v zapisu 4.3, prav tako ne moremo potrditi, da gre za škodljivo sporočilo.

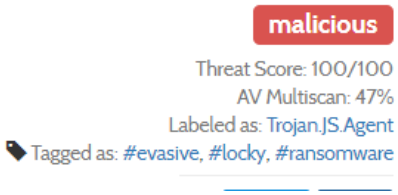
Zapis 4.3 Zapis vsebine prejetega sporočila.

```
Dear Sir,

Please find attached POs for your reference.
Invoice name and address should be mentioned as in the PO.
Please send us the Proforma Invoices for both POs (Air freight and sea freight) separately.

Regards,
JELENA MARTINEZ|SALES DEPARTMENT
TEHNO PRODUCTS EXPORT D.O.O.
Jabucki put 221|PAK302917 26101 Pancevo|Serbia
Tel: ++ 381 13 334507|Fax: ++ 381 13 377564|Cell: ++ 381 69 8479060
Skype: jelenamart
 Virus-free. www.avg.com
```

Kot zadnje orodje, ki nam lahko da potrditev, da gre za škodljivo datoteko, smo uporabili spletno stran www.hybrid-analysis.com, na katero smo prenesli datoteko iz sporočila. Po izvedeni analizi smo prejeli potrditev, da gre za škodljvo priponko, kot je prikazano na sliki 4.31. Dodatno nam spletna stran prikaže tudi škodljive aktivnosti, ki se izvedejo na sistemu, na katerem odpremo datoteko in so prikazane v zapisu 4.4.



Slika 4.30 Pregled IP naslova pošiljatelja na spletni strani Talos.



Slika 4.31 Rezultat analize datoteke na spletni strani Payload Security.

Zapis 4.4 Povzetek tehnične analize škodljive datoteke.

```
Remote Access: Reads terminal service related keys (often RDP related)
Spyware: Accesses potentially sensitive information from local browsers POSTs files to a
    webserver
Fingerprint: Reads the active computer name Reads the cryptographic machine GUID
Evasive: Executes WMI queries known to be used for VM detection
Exploit: Contains escaped byte string (often part of obfuscated shellcode)
Spreading: Opens the MountPointManager (often used to detect additional infection locations)
Network Behavior: Contacts 11 domains and 5 hosts. View the network section for more details.
```

Po končani celoviti analizi smo spoznali način in posledice okužbe. Preko zapisov smo lahko preverili ali so bila iz istega naslova poslana sporočila tudi drugim internim prejemnikom. Po končani analizi smo lahko pripravili tudi dodatne varnostne ukrepe, kako zmanjšati možnost okužb. V konkretnem primeru se je pri dostavi kriptirane pošte končnemu uporabniku dodalo obvestilo o pravilnem rokovanju s takšno pošto. Dodatno se je pripravilo izobraževanje iz področja varnosti za zaposlene.

5 Zaključek

Informacijska varnost je čedalje bolj pomembna za delovanje in tudi obstoj organizacij. Zaradi tega se v informacijskem okolju srečamo s številnimi različnimi varnostnimi rešitvami in različnimi politikami ali predpisi. Posledica tega je množica zapisov, ki jih naprave zapisujejo na različna mesta v različnih oblikah. V manjših okoljih je z analitičnim delom varnostnega inženirja še možno pridobiti in povezati informacije iz različnih virov brez uporabe namenske programske rešitve, že v malo večjih okoljih pa je zaradi prevelikega števila zapisov in raznolikosti sistemov to nemogoče. Tam centralno vlogo pri varnosti informacijskega sistema prevzame SIEM, ki zagotavlja celovitost informacij, integriteto in normalizacijo zapisov ter povezovanje zapisov iz različnih virov za odkrivanje kompleksnih napadov. Postavitev SIEM sistema v neko okolje je kompleksen proces. Eden od ciljev diplomske naloge je prikaz popisa naprav in postopkov integracije le teh v SIEM sistem. Gre za analitičen proces, ki lahko zahteva veliko časa in poznavanje lastnosti različnih sistemov. Rezultat tega procesa je centralizirano mesto za beleženje zapisov in centraliziran pregled nad dogodki zbranimi iz različnih naprav. Drugi cilj diplomske naloge je prikaz uporabe SIEM sistema. Gre za prikaz možnosti priprave prilagojenih

pogledov, ki so prirejeni vlogi uporabnika v informacijskem sistemu in prikaz vrtanja v globino, ki omogoča uporabniku SIEM sistema enostavno pridobivanje dodatnih informacij o zaznanih dogodkih. Tretji cilj diplomske naloge je prikaz treh tipičnih analiz, ki jih skrbniki izvajajo v SIEM sistemu. Prikazana je prednost centralnega zbiranja zapisov in možnost iskanja dogodkov iz zapisov posredovanih s strani različnih sistemov. Proces izvajanja analiz in odkrivanje novih korelacij sta opravili, ki se nikoli ne zaključita. Z uvajanjem novih tehnologij se namreč pojavijo nova tveganja, na katera odgovorimo z novimi varnostnimi rešitvami, ki posredujejo nove zapise. Te zapise moramo vključiti v nove analize in korelacije.

Vloga SIEM sistemov v informacijskem okolju se je tekom let povečevala. Z razvojem različnih programsko definiranih rešitev (angl. *software defined*) pa se bo vloga SIEM sistemov še povečala, saj ta tehnologija omogoča dvosmerno izmenjavo podatkov med sistemi. S tem bo SIEM sistem lahko dajal navodila ostalim napravam, da blokirajo nek promet ali izolirajo nek sistem iz omrežja.

Literatura

[1] Margaret Rouse, Ivy Wigmore, Definition log (log file), November 2014. [Elektronski]. Dostopno na: http://whatis.techtarget.com/definition/log-log-file. [Poizkus dostopa 22.4.2017].

[2] Cisco IOS Configuration Fundamentals Configuration Guide, Release 12.2; Chapter: Troubleshooting, Fault Management, and Logging, 2004

[3] Desktop Operating System Market Share, Marec 2017 [Elektronski]. Dostopno na: https://www.netmarketshare.com/operating-system-market-share.aspx. [Poizkus dostopa 14.4.2017].

[4] Usage share of operating systems, Public servers on the Internet, April 2017 [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/Usage_share_of_operating_systems. [Poizkus dostopa 14.4.2017].

[5] Web Server, April 2017 [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/Web_server. [Poizkus dostopa 14.4.2017].

[6] Borut Breščak, Projekt računalniške komunikacije in omrežja, Stikala, 2006 [Elektronski]. Dostopno na: http://www.s-sers.mb.edus.si/gradiva/w3/omrezja/32_podaljsevanje/switch.html. [Poizkus dostopa 25.4.2017].

[7] Wireshark, [Elektronski]. Dostopno na: https://www.wireshark.org/. [Poizkus dostopa 25.4.2017].

[8] NetFlow, April 2017 [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/NetFlow. [Poizkus dostopa 27.4.2017].

[9] Specification of the IP Flow Information Export (IPFIX). Protocol for the Exchange of Flow InformationNetFlow, September 2013 [Elektronski]. Dostopno na: https://tools.ietf.org/html/rfc7011. [Poizkus dostopa 27.4.2017].

[10] Cisco IOS Flexible NetFlow Flow Monitors and collection of the export data, Junij 2006 [Elektronski]. Dostopno na: http://www.cisco.com/c/en/us/products/collateral/ios-nx-os-software/flexible-netflow/product_data_sheet0900aecd804b590b.html. [Poizkus dostopa 27.4.2017].

[11] Talos - The world's largest Email and Web traffic monitoring network [Elektronski]. Dostopno na: https://talosintelligence.com/. [Poizkus dostopa 23.7.2017].

[12] File Content Security Datasheet [Elektronski]. Dostopno na: https://www.fireeye.com/products/fx-content-security-products/fx-file-content-security-datasheet.html. [Poizkus dostopa 3.5.2017].

[13] virustotal [Elektronski]. Dostopno na: https://www.virustotal.com/. [Poizkus dostopa 6.5.2017].

[14] VxStream Sandbox - Automated Malware Analysis System[Elektronski]. Dostopno na: https://www.payload-security.com/products/vxstream-sandboxl. [Poizkus dostopa 6.5.2017].

[15] Saleem Kazmi, "Centralized Logging using Logsentry in a Large UNIX Environment",SANS Institute, September 2002. [Elektronski]. Dostopno na: https://www.giac.org/paper/gsec/2256/centralized-logging-logsentry-large-unix-environment/103878. [Poizkus dostopa 10.5.2017].

[16] Joe Piggeé Sr., What Is a SIEM?, Januar 2016. [Elektronski]. Dostopno na: https://www.tripwire.com/state-of-security/incident-detection/log-management-siem/what-is-a-siem/. [Poizkus dostopa 10.5.2017].

[17] Mike Rothman, The Past, Present and Future of SIEM, Julij 2014. [Elektronski]. Dostopno na: http://searchsecurity.techtarget.com/video/The-past-present-and-future-of-SIEM-technology/. [Poizkus dostopa 16.5.2017].

[18] RSA, Advanced Cyber Defence, 2017 [Elektronski]. Dostopno na: https://ireland.emc.com/services/rsa-services/advanced-cyber-defense/threat-landscape.htm. [Poizkus dostopa 3.6.2017].

[19] Kif Leswing, Yahoo confirms major breach — and it could be the largest hack of all time, September 2016. [Elektronski]. Dostopno na: http://uk.businessinsider.com/yahoo-hack-by-state-sponsored-actor-biggest-of-all-time-2016-9?r=US&IR=T. [Poizkus dostopa 3.6.2017].

[20] Rohit Malhotra, RSA NetWitness Suite, Marec 2017 [Elektronski]. Dostopno na: https://www.slideshare.net/dynamiccio/detect-unknown-threats-reduce-dwell-time-accelerate-response. [Poizkus dostopa 8.9.2017].

[21] McAfee ESM, Data Source Configuration, 2017 [Elektronski]. Dostopno na: https://kc.mcafee.com/resources/sites/MCAFEE/content/live/PRODUCT_DOCUMENTATION/26000/PD26993/en_US/esm_data_source_rg_rev_a_en-us.pdf. [Poizkus dostopa 21.5.2017].

[22] SIEM Event Log Collection Methods: Agent vs. Agent-Less. [Elektronski]. Dostopno na: http://www.snarealliance.com/siem-event-log-collection-methods-agent-vs-agent-less/. [Poizkus dostopa 21.5.2017].

[23] Asaf Yigal, How to Build a SIEM Dashboard for AWS Using the ELK Stack, April 2016 [Elektronski]. Dostopno na: https://logz.io/blog/siem-dashboard-aws-elk-stack/. [Poizkus dostopa 29.5.2017].

[24] Data link layer, Junij 2017. [Elektronski]. Dostopno na: https://en.wikipedia.org/wiki/Data_link_layer. [Poizkus dostopa 22.8.2017].

[25] What is a Virtual LAN (VLAN)?, Avgust 2017. [Elektronski]. Dostopno na: https://www.lifewire.com/virtual-local-area-network-817357. [Poizkus dostopa 22.8.2017].

[26] Randy Franklin Smith, Windows Security Log ID [Elektronski]. Dostopno na: https://www.ultimatewindowssecurity.com/securitylog/encyclopedia/event.aspx?eventID=4624. [Poizkus dostopa 24.8.2017].

[27] Mark Maiville,2016 Gartner Magic Quadrant for SIEM, November 2016. [Elektronski]. Dostopno na: https://www.idrgrp.com/magic-quadrant-2016/. [Poizkus dostopa 3.6.2017].

[28] Victor Bueno, Demo presentation McAfee SIEM, September 2016. [Elektronski]. Dostopno na: https://www.slideshare.net/vbueno/presentacion-demo-mcafee-siem-65701740. [Poizkus dostopa 15.9.2017].